Додаток
до розпорядження голови
районної в місті ради
від 14.11.2017 № 251-р

Настанова
з інформаційної безпеки виконкому
Довгинцівської районної в місті ради

Зміст

1. Вступ 2
2 Сфера застосування 2
3. Нормативні посилання 3
4. Система управління інформаційною безпекою 4
4.1. Загальні положення 4
4.2. Управління системи управління інформаційною безпекою 4
4.2.1 Планування системи управління інформаційною безпекою 4
4.2.1.1 Політика в сфері інформаційної безпеки 4
4.2.1.2. Оцінка ризиків 5
4.2.1.3. Положення про застосовність 6
4.2.2 Упровадження заходів безпеки, процесів та процедур системи керування інформаційною безпекою 6
4.2.2.1 Планування оброблення ризиків 6
4.2.2.2. Процеси інформування 7
4.2.3 Процедура моніторингу та контролю 7
4.2.4 Перегляд ефективності системи управління інформаційною безпекою 8
4.3. Управління документацією 8
4.3.1 Загальні положення 8
4.3.2 Контроль документів 10
4.3.3 Контроль записів 11
5. Відповідальність керівництва 11
5.1. Зобов’язання керівництва 11
5.2. Управління ресурсами 12
5.2.1 Забезпечення ресурсами 12
5.2.2 Навчання, поінформованість та компетентність 13
6. Моніторинг, вимірювання, аналіз та оцінка 13
7. Перегляд системи управління інформаційною безпекою керівництвом 15
8. Удосконалення системи управління інформаційною безпекою 15
8.1. Постійне вдосконалення 15
8.2. Процедури реагування на інциденти безпеки здійснення коригувальних і запобіжних дій 16
Додаток 18

1. Вступ

Виконавчий комітет Довгинцівської районної в місті ради (далі – виконком) є виконавчим органом районної в місті ради, утворюється радою на строк її повноважень, підзвітний і підконтрольний їй, а з питань здійснення делегованих повноважень органів виконавчої влади – підконтрольний відповідним органам виконавчої влади.

Виконком є юридичною особою, має печатку зі своїм найменуванням, рахунки в установах банків України, може від свого імені набувати майнових і особистих немайнових прав, бути позивачем і відповідачем у суді та мати інші повноваження в межах чинного законодавства України. Виконком у своїй роботі керується Положенням про виконавчий комітет Довгинцівської районної в місті ради та Регламентом.

Діє виконком у межах повноважень, визначених Законом України «Про місцеве самоврядування в Україні» та іншими законодавчими актами України, рішенням Криворізької міської ради від 31.03.2016 № 381 «Про обсяг і межі повноважень районних у місті рад та їх виконавчих органів» зі змінами.

Очолює та здійснює керівництво виконкомом голова районної в місті ради, а в разі його відсутності чи неможливості здійснення ним цих функцій посадова особа, яка виконує його обов’язки.

Утворені районною в місті радою структурні підрозділи виконкому підпорядковуються голові районної в місті ради, його заступникам та керуючому справами відповідно до розподілу обов’язків. Їх керівники та посадові особи виконкому призначаються на посаду й звільняються з неї головою районної в місті ради одноособово.

Робота виконкому, його структурних підрозділів є відкритою і прозорою. У встановленому порядку здійснюється доступ до публічної інформації про діяльність районної в місті ради, її виконавчого комітету, крім інформації з обмеженим доступом.

Контактна інформація:

Адреса: Україна, 50086, Дніпропетровська область, місто Кривий Ріг, Довгинцівський район, вулиця Дніпровське шосе, 11.

Телефон: +380 (564) 711329.

Факс: +380 (564) 715136.

E-mail: dlgr@dlgr.gov.ua.

2 Сфера застосування

Система управління інформаційною безпекою (далі - СУІБ) виконкому впроваджена розпорядженням голови районної в місті ради відповідно до вимог ДСТУ ISO/IEC 27001:2015.

Метою розробки та впровадження системи управління інформаційною безпекою є забезпечення вибору необхідних засобів управління захистом, що

захищають інформаційні активи та надають упевненості зацікавленим сторонам у їх схоронності.

СУІБ розповсюджується на процеси виконавчих функцій та делегованих повноважень органу місцевого самоврядування (рішення Криворізької міської ради від 31.03.2016 № 381 «Про обсяг і межі повноважень районних у місті рад та їх виконавчих органів» зі змінами).

СУІБ виконкому в якості вхідних даних бере вимоги захисту інформації й очікування зацікавлених сторін та через необхідні дій і процеси видає результати захисту інформації, що задовольняють цим вимогам і очікуванням.

Дія системи управління інформаційною безпекою розповсюджується на всі структурні підрозділи виконкому.

Виконком не встановлює цілі заходів безпеки стосовно здійснення електронної комерції (А. 10.9.1 ДСТУ ISO/IEC 27001:2015), інтерактивних трансакцій (А. 10.9.2 ДСТУ ISO/IEC 27001:2015), мобільних обчислень та дистанційної роботи (А.11.7 ДСТУ ISO/IEC 27001:2015), оскільки ці процеси фактично відсутні.

3. Нормативні посилання

Настанова з інформаційної безпеки виконкому містить посилання на наступні нормативні документи:

- ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2015, IDT);
- Закон України «Про місцеве самоврядування в Україні»;
- Закон України «Про захист персональних даних»;
- Закон України «Про інформацію»;
- Закон України «Про доступ до публічної інформації»;
- Постанова Кабінету Міністрів України від 30 листопада 2011 року №1242 «Про затвердження Типової інструкції з діловодства у центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади»;
- Рішень Криворізької міської ради від:
- 31.03.2016 № 381 «Про обсяг і межі повноважень районних у місті рад та їх виконавчих органів» зі змінами;
- 08.12.2012 № 71 «Про затвердження Інструкції з діловодства в органах місцевого самоврядування міста» зі змінами;
- рішення виконкому районної в місті ради від:
- 21.11.2012 № 702 «Про затвердження Положення про захист персональних даних у базах персональних даних, володільцем яких є виконком районної в місті ради» зі змінами;
- 15.06.2016 № 204 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.

4. Система управління інформаційною безпекою

4.1. Загальні положення

Для функціонування системи управління інформаційною безпекою встановлено такі групи процесів (видів діяльності), що використовуються на всіх рівнях виконкому:

- процеси керування у сфері відповідальності керівництва;
- допоміжні процеси забезпечення ресурсами;
- основні процеси впровадження заходів інформаційної безпеки;
- процеси моніторингу та вимірювань.

Процеси системи управління інформаційною безпекою взаємопов'язані та виконуються послідовно відповідно до циклу Шухарта-Демінга, який застосовується для структуризації всіх процесів системи управління інформаційною безпекою.

Процеси характеризуються наявністю:

- постачальника;
- власника;
- споживача;
- вхідних та вихідних даних;
- ресурсів, необхідних для виконання;
- критеріїв моніторингу і контролю;
- відповідальних за виконання.

Виконком направляє СУІБ на задоволення вимог (в тому числі очікувань) своїх зацікавлених сторін:

- громадськість району;
- органів державної влади.

Задокументована СУІБ виконкому є доступною, її вимоги обов'язкові для персоналу структурних підрозділів виконкому. У свою чергу персонал виконкому повинен забезпечувати ефективне виконання документованих процедур та інструкцій системи керування інформаційною безпекою.

4.2. Управління системи управління інформаційною безпекою

4.2.1 Планування системи управління інформаційною безпекою

4.2.1.1 Політика в сфері інформаційної безпеки

Розпорядженням голови районної у місті ради від 09.11.2017 № 241-р затверджено Політику у сфері інформаційної безпеки виконкому Довгинцівської районної в місті ради. Вона розроблена відповідно до вимог чинного законодавства України, ДСТУ ISO/IEC 27001:2015 та визначає місію, пріоритети та принципи діяльності виконкому в сфері інформаційної безпеки й основні шляхи їх реалізації.

Працівники структурних підрозділів виконкому повинні бути ознайомлені з Політикою у сфері інформаційної безпеки виконкому та забезпечувати її реалізацію.

Через авторизовані канали, зокрема через офіційний сайт виконкому, інформація про політику доводиться до зацікавлених сторін; є можливість звернутися до головного уповноваженого з питань СУІБ виконкому для ознайомлення із Політикою.

Політика в сфері інформаційної безпеки переглядається за потребою, але не рідше одного разу на рік. Пропозиції щодо внесення змін та доповнень до Політики в сфері інформаційної безпеки подаються посадовою особою виконкому відповідальною за функціонування системи управління інформаційною безпекою, на розгляд головному уповноваженому з питань СУІБ виконкому.

Відповідно до Політики в сфері інформаційної безпеки встановлюються цілі заходів безпеки та заходи безпеки для оброблення ризиків.

Цілі інформаційної безпеки повинні:

- перебувати у відповідності з Політикою в сфері інформаційної безпеки;
- бути вимірними (якщо це можливо);
- брати до уваги чинні вимоги інформаційної безпеки, результати перевірок та обробки ризиків;
- бути відомі відповідному персоналу організації;
- оновлюватися по мірі необхідності.

Організація повинна зберігати документовану інформацію про цілі інформаційної безпеки.

При плануванні заходів по досягненню своїх цілей інформаційної безпеки виконком визначає:

- заходи;
- ресурси;
- відповідальність;
- термін реалізації заходів;
- методи оцінювання результатів.

4.2.1.2. Оцінка ризиків

Виявлення й оцінка ризиків інформаційної безпеки відбувається відповідно до «Методики управління ризиками». Основними її завданнями є:

- установлення ефективної підтримки прийняття управлінських рішень з урахуванням рівня ризиків у сфері інформаційної безпеки;
- забезпечення здійснення діяльності виконкому у відповідності до встановлених політик, процедур і регламентів;
- зниження рівня очікуваних і неочікуваних ризиків.

Методологія управління ризиками базується на відповідних законодавчих та нормативних вимогах щодо захисту інформації. Методика встановлює критерії оцінки та прийняття ризиків, а також визначає прийнятні їх рівні.

Перелік ризиків документується та погоджується керівництвом виконкому. Форма документування регламентована Методикою управління ризиками. Погоджені ризики вважаються прийнятими.

Ризики інформаційної безпеки, що прийняті, але за ними не плануються заходи безпеки (залишкові ризики) погоджуються керівництвом окремо з обґрунтуванням їх прийняття та строками впровадження заходів безпеки.

Оцінка ризиків передбачає визначення:

- ступеня ймовірності їх виникнення;
- можливих негативних наслідків;
- рівня загрози виникнення ризику, що може вплинути на виконання функціональних обов'язків і процесів, обсяг можливих збитків.

Перегляд оцінки ризиків відбувається не рідше 1 разу на рік, або в разі:

- виникнення інциденту у сфері інформаційної безпеки;
- упровадження нових або вилучення існуючих процесів.

4.2.1.3. Положення про застосовність

У залежності від існуючих процесів, законодавчих та нормативних вимог, ризиків інформаційної безпеки у виконкомі визначаються цілі заходів інформаційної безпеки та заходи обробки ризиків. Цілі документуються у вигляді Положення про застосовність цілей заходів інформаційної безпеки. Положення містить цілі та засоби управління, виключення цілей управління та їх обґрунтування.

4.2.2 Упровадження заходів безпеки, процесів та процедур системи керування інформаційною безпекою

4.2.2.1 Планування оброблення ризиків

Вхідними даними для планування оброблення ризиків є:

- законодавчі та нормативні вимоги;
- Політика в сфері інформаційної безпеки;
- цілі керування інформаційною безпекою;
- рішення щодо залишкових ризиків;
- аналіз даних нагляду за виконанням процесів СУІБ;
- інформація щодо ресурсів (персоналу, інфраструктури, виробничого середовища, матеріалів, технічних засобів тощо);
- виявлені можливості для вдосконалення.

Вихідними даними планування оброблення ризиків є рішення щодо:

- розробки правил та політики управління інформацією, зокрема документами;
- здійснення заходів з обробки ризиків, зокрема щодо зменшення або уникнення ризиків інформаційної безпеки;
- розподілу повноважень і відповідальності;
- розвитку інфраструктури та ресурсної бази;
- забезпечення компетентним персоналом.

Перегляд планів упровадження заходів безпеки відбувається не рідше 1 разу на рік, або в разі:

- виникнення інциденту інформаційної безпеки;

- вилучення або впровадження нових процесів.

Аналіз ефективності заходів безпеки здійснює посадова особа, відповідальна за функціонування СУІБ.

4.2.2.2. Процеси інформування

Голова районної в місті ради, його заступники та керівники структурних підрозділів виконкому встановлюють і забезпечують наявність результативних процесів обміну інформацією, пов'язаною з діяльністю виконкому та результативністю СУІБ. Вимоги до обміну інформацією встановлено Регламентом, затвердженим рішенням районної в місті ради від 19.02.2016 № 24 «Про затвердження Регламенту Довгинцівської районної в місті ради».

У виконкомі використовуються такі методи внутрішнього та зовнішнього інформування:

- видача рішень районної в місті ради та її виконкому, розпоряджень голови районної в місті ради;
- розповсюдження копій документів на паперових та електронних носіях;
- розповсюдження інформації через офіційний веб-сайт виконкому районної в місті ради, на сайті «Криворізький ресурсний центр» у мережі Інтернет;
- в локальній комп'ютерній мережі;
- розміщення інформації в засобах масової інформації;
- представлення інформації на нарадах у керівництва чи зборах колективу;
- розміщення інформації на стендах.

Керівники структурних підрозділів виконкому в межах своїх повноважень несуть відповідальність за додержання персоналом професійної таємниці щодо інформації, яку вони отримують у результаті виконаних робіт від суб'єктів господарювання, громадян.

Загальні вимоги щодо забезпечення конфіденційності доводяться до всього персоналу виконкому. Усі документи та інформація, що надійшли від суб'єктів господарювання, громадян не повинні передаватися третій особі без письмової їх згоди.

Виконком несе відповідальність за належне збереження інтелектуальної власності замовника відповідно до чинного законодавства України, повинен не допускати незаконного розповсюдження інформації, документів, матеріалів чи інших предметів, наданих замовником (громадянином) для опрацювання (послуга, процес, перевірка, затвердження тощо).

4.2.3 Процедура моніторингу та контролю

У виконкомі здійснюється контроль за діями персоналу, роботою програмного забезпечення тощо. Оперативний контроль виконавчої дисципліни, дотримання встановлених процедур та внутрішній аудит СУІБ здійснюються від-

повідно до вимог чинного законодавства України. Вимоги до методів здійснення контролю викладені в Регламенті виконавчого комітету районної в місті ради, Настанові з інформаційної безпеки, розпорядженнях голови районної в місті ради з питань інформаційної безпеки. Вимоги направлені на виявлення та термінове реагування на інциденти інформаційної безпеки, помилки в результаті обробки інформації, підвищення продуктивності діяльності щодо забезпечення інформаційної безпеки, подій безпеки, оцінку ефективності дій з усунення порушень безпеки.

4.2.4 Перегляд ефективності системи управління інформаційною безпекою

Для здійснення перегляду ефективності впровадженої СУІБ виконкомом районної в місті ради впроваджуються та підтримуються процеси моніторингу, вимірювань, аналізу й поліпшення інформаційної безпеки.

Вони спрямовані на:

- створення відкритих, зручних і доступних умов для отримання якісних адміністративних послуг мешканцями району;
- забезпечення відповідності СУІБ виконкому районної в місті ради вимогам ДСТУ ISO/IEC 27001:2015;
- постійне поліпшення діяльності СУІБ.

Ці процеси полягають в одержанні, обробці та узагальненні інформації про функціонування СУІБ, їх ефективності та розробці необхідних заходів щодо її поліпшення, включаючи коригувальні й запобіжні дії.

4.3. Управління документацією

4.3.1 Загальні положення

З метою забезпечення функціонування та розвитку СУІБ у виконкомі районної в місті ради розробляється та впроваджується документація:

- Політика в сфері інформаційної безпеки;
- Настанова з інформаційної безпеки;
- Положення про застосовність;
- переліки інформаційних активів і ризиків;
- методика управління ризиками;
- процедури та протоколи, що підтверджують реалізацію функцій і вимог системи управління інформаційною безпекою;
- інші документи, на які є посилання в процедурах та інструкціях.

Об’єм документів, які необхідні для результативного функціонування СУІБ та забезпечення зворотного зв’язку засобів управління з результатами процесів оцінювання й обробки ризиків, а також політикою та цілями СУІБ, встановлюється в залежності від:

- розмірів організації;
- сфери розповсюдження СУІБ;
- видів діяльності, які здійснює виконком;
- складності вимог щодо безпеки.

Рекомендований перелік документів СУІБ вказаний у додатку до Настанови з інформаційної безпеки виконкому Довгинцівської районної в місті ради.

Документи можуть існувати в будь-якій формі та на будь-якому носії, але необхідно враховувати обов'язкові законодавчі та нормативні вимоги щодо форми та типу носія, а також ризики, пов'язаній із забезпеченням доступності та цілісності.

Записи визначаються, як документи особливого типу, які призначені для забезпечення доказової бази або для прослідковування тенденцій змін в СУІБ. Керування записами здійснюється відповідно до п. 4.3.2 цієї Настанови СУІБ та процедурі «Управління записами».

Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради (надалі - Настанова з інформаційної безпеки) - це опис функціонування СУІБ у виконкомі та є його власністю. Вона встановлює цілі, задачі та принципи функціонування СУІБ, розподіл повноважень і відповідальності серед керівників та працівників структурних підрозділів виконкому районної в місті ради на всіх етапах виконання управлінських та контрольних функцій.

Настанова з інформаційної безпеки призначена для використання в цілях:

- забезпечення стабільного функціонування СУІБ, її самооцінки та вдосконалення;
- підготовки персоналу для виконання робіт відповідно до вимог СУІБ;
- забезпечення необхідної інформації при проведенні перевірок СУІБ;
- інформування зацікавлених сторін (громадян, суб'єктів господарювання тощо) про політику та процедури виконкому районної в місті ради в сфері інформаційної безпеки.

Настанова з інформаційної безпеки розповсюджується на всі процеси, пов'язані з інформаційною безпекою, встановлює вимоги до функціонування системи керування нею, документально підтверджує політику та процедури. У Настанові з інформаційної безпеки застосовуються терміни та визначення, установлені ДСТУ ISO/IEC 27001.

Положення Настанови з інформаційної безпеки обов'язкові для виконання при здійсненні дій з інформаційними активами. Зареєстровані копії Настанови призначені для внутрішнього користування. Використовувати в роботі її незареєстровані копії забороняється.

Термін дії Настанови з інформаційної безпеки необмежений, її зміст переглядається та вдосконалюється за потребою.

У разі, якщо на думку будь-якого співробітника окремі положення Настанови з інформаційної безпеки або вона в цілому не відповідають у повній мірі вимогам щодо забезпечення належного рівня функціонування СУІБ, він має право звернутися до уповноваженого з питань розробки та впровадження системи управління інформаційною безпекою у виконкомі районної в місті ради або посадової особи, відповідальної за функціонування СУІБ з пропозицією про проведення її коригування.

Рішення про перегляд та коригування Настанови з інформаційної безпеки приймає уповноважений з питань розробки та впровадження системи управління інформаційною безпекою у виконкомі районної в місті ради.

Облік документів СУІБ ведуть особи, відповідальні за функціонування СУІБ, а зберігаються у розробників або у тих, хто веде записи.

4.3.2 Контроль документів

Контролювання документами СУІБ має здійснюватися для забезпечення:

- доступності та придатності для використання в місцях, де вона необхідна;
- адекватного захисту (наприклад, від втрати конфіденційності, неправильного використання або втрати цілісності).

Для управління документованої інформацією виконком повинен розглядати наступні заходи (якщо застосовно):

- поширення інформації, доступ, відновлення та використання;
- зберігання та схоронність, у тому числі збереження зручності для читання;
- контроль змін (наприклад, управління версіями);
- архівування та знищення.

Документована інформація зовнішнього походження, яка необхідна для планування і функціонування СУІБ, повинна бути визначена відповідним чином.

Виконком районної в місті ради здійснює управління документацією СУІБ на підставі Регламенту, затвердженого рішенням районної в місті ради від 19.02.2016 № 24 «Про затвердження Регламенту Довгинцівської районної в місті ради», який визначає принципи та порядок:

1) організації:
- роботи зі службовими документами;
- контролю за виконанням нормативно-правових актів, розпорядчих документів районної в місті ради, її виконкому та голови районної в місті ради;
- використання фірмових бланків, гербових печаток та печаток без зображення герба;

2) забезпечення:
- наявності відповідних версій чинних документів у місцях застосування;
- ідентифікації змін та статусу чинної версії документів;
- контролю за розповсюдженням документів;

3) роботи:
- зі скаргами, заявами, зверненнями, пропозиціями та інформаційними запитами;
- з єдиним електронним реєстром документів виконкому;
- у локальній комп’ютерній мережі виконкому районної в місті ради та з електронною поштою;
- щодо запобігання ненавмисному застосуванню застарілих документів;
- розміщення матеріалів на офіційному веб-сайті виконкому районної в місті ради в мережі Інтернет;

- формування номенклатури справ у загальному відділі виконкому, тимчасовому зберіганню та використанню архівних документів;
- взаємодії із засобами масової інформації та громадськістю.

Вимоги до документації системи управління якістю та СУІБ виконкому викладені в Інструкції з діловодства в органах місцевого самоврядування міста, затвердженій рішенням виконавчого комітету Криворізької міської ради від 08.02.2012 № 71 та процедурі «Порядок управління документацією».

4.3.3 Контроль записів

Для результативної реалізації функцій та вимог СУІБ виконкомом районної в місті ради впроваджуються та ведуться протоколи, які фіксують факт події в сфері інформаційної безпеки або її результати.

До протоколів належать всі форми документування даних стосовно інформаційної безпеки, результатів контролю та аналізу.

Управління протоколами здійснюється відповідно до процедури «Управління записами» на етапах:

- розробки форми;
- упровадження протоколу;
- унесення даних;
- зберігання протоколу.

Записи повинні бути захищені від втрати, знищення, фальсифікації, неавторизованого доступу та неавторизованого випуску, відповідно до законодавчих, нормативних та договірних вимог.

5. Відповідальність керівництва

5.1. Зобов'язання керівництва

Голова районної в місті ради демонструє лідерство і прихильність по відношенню до СУІБ шляхом:

- забезпечення політики та цілей інформаційної безпеки, які розроблені і сумісні зі стратегічними завданнями виконкому;
- забезпечення інтеграції вимог СУІБ в процеси організації;
- забезпечення того, щоб ресурси, необхідні для СУІБ, були доступні;
- інформування про важливість досягнення результативності управління інформаційної безпеки і про відповідність вимогам СУІБ;
- забезпечення того, що СУІБ дозволяє досягати бажаних результатів;
- підтримки й управління персоналом, який сприяє підвищенню результативності СУІБ;
- сприяння постійному поліпшенню;
- підтримки інших відповідних ролей управління з метою демонстрації ними лідерських якостей у застосуванні до сфери їх відповідальності.

Для організації роботи СУІБ розпорядженням голови районної в місті ради призначаються уповноважений з питань розробки та впровадження системи управління інформаційною безпекою у виконкомі районної в місті ради, поса-

дова особа виконкому районної в місті ради відповідальна за функціонування СУІБ у виконкомі районної в місті ради та посадові особи, відповідальні з питань інформаційної безпеки у структурних підрозділах виконкому районної в місті ради.

Повноваження щодо координації роботи з питань інформаційної безпеки покладаються на уповноваженого з питань розробки та впровадження системи управління інформаційною безпекою, який призначається з числа заступників голови районної в місті ради або керуючий справами виконкому; контроль за процесами, що забезпечують функціонування СУІБ покладається на посадову особу виконкому районної в місті ради відповідальну за функціонування СУІБ. У кожному структурному підрозділі виконкому районної в місті ради призначаються посадові особи, відповідальні за інформаційну безпеку, які наділені відповідними обов'язками, відповідальністю та повноваженнями.

5.2. Управління ресурсами

5.2.1 Забезпечення ресурсами

Діяльність щодо забезпечення ресурсами спрямована на:

- створення, упровадження, використання, постійний контроль, аналізування, підтримку в робочому стані та поліпшення СУІБ;
- гарантування направленості процедур захисту інформації на виконання вимог чинного законодавства України в сфері інформаційної безпеки, стандарту ДСТУ ISO/IEC 27001;
- виявлення та розгляд нормативних і законодавчих вимог та договірних зобов'язань щодо захисту інформаційних активів;
- проведення аналізу функціонування СУІБ та реагування на його результати;
- поліпшення результативності СУІБ.

До ресурсів належать:

- персонал виконкому районної в місті ради;
- робоче середовище;
- інфраструктура;
- фінанси.

З метою підтримання системного підходу до керування ІБ та оперативного реагування на інциденти у виконкомі створюються комунікативні канали.

Для реалізації вимог СУІБ у виконкомі проводиться управління документами, що передбачає забезпечення регламентними документами виконавців та фіксування важливої інформації.

Планування ресурсів здійснюється в рамках планування діяльності, розвитку та матеріально-технічного забезпечення виконкому районної в місті ради.

При цьому вирішуються питання:

- планування потреб у ресурсах;
- забезпечення необхідними матеріальними та нематеріальними (інтелектуальними) ресурсами;
- забезпечення персоналом, підтримка та підвищення його кваліфікації;

- розвиток інфраструктури.

5.2.2 Навчання, поінформованість та компетентність

Реалізація проголошеної Політики в сфері інформаційної безпеки та досягнення поставлених завдань розвитку здійснюються через:

- визначення вимог до компетентності посадових осіб (персоналу виконкому (посадових осіб, спеціалістів та робітників), їх обов'язків і повноважень;
- забезпечення професійної підготовки та постійної підтримки кваліфікації посадових осіб;
- доведення до працівників Політики в сфері інформаційної без-пеки та поставлених завдань, оперативної інформації та значимості їх діяльності в галузі захисту інформації, їх вкладу в досягнення цілей СУІБ, наслідків недотримання вимог СУІБ;
- оцінки результативності (або ефективність) дій по навчанню, інформуванню тощо.

Процедурні питання щодо управління компетентністю регламентуються вимогами п. 6.2.2. Настанови щодо якості виконавчого комітету Довгинцівської районної в місті ради.

Підвищення кваліфікації працівників виконкому здійснюється через навчання у відповідних навчальних закладах раз на п'ять років та шляхом:

- отримання другої вищої освіти;
- підвищення кваліфікації на базі Дніпропетровського регіонального інституту державного управління Національної академії державного управління при Президентові України;
- внутрішнього навчання;
- участі в роботі профільних семінарів і конференцій тощо.

Уся інформація про професійну підготовку спеціалістів, набутий досвід роботи та використані види навчання міститься в персональних справах співробітників, які зберігаються в відділі з питань кадрової роботи виконкому районної в місті ради.

6. Моніторинг, вимірювання, аналіз та оцінка

Виконавчий комітет оцінює стан інформаційної безпеки та результативність СУІБ шляхом оперативного моніторингу, спостереження та аудиту СУІБ, аналізування та оцінки результативності СУІБ. Вибрані методи повинні виробляти зіставні та відтворювані результати, які будуть достовірними.

Виконавчий комітет визначає:

- предмет відстеження і вимірювання, в тому числі процеси інформаційної безпеки та елементи управління;
- методи моніторингу, вимірювання, аналізу та оцінки, в залежності від обставин, в цілях забезпечення достовірних результатів;
- періодичність моніторингу та вимірювань;
- відповідальних та виконавців моніторингу і вимірювання;

- час аналізування та оцінювання результатів моніторингу та вимірювань;
- відповідальних та виконавців аналізування і оцінювання результатів.

Документована інформація, яка підтверджує результати моніторингу та вимірювань, має передаватися та зберігатися під контролем уповноваженого з питань розробки та впровадження системи управління інформаційною безпекою.

Порядок проведення внутрішніх аудитів СУІБ регламентується Процедурою «Порядок проведення внутрішніх аудитів».

Метою внутрішнього аудиту є здійснення підтримки відповідності СУІБ виконкому районної в місті ради вимогам нормативних доку-ментів, своєчасне виявлення відхилень, недоліків і розробка заходів щодо їх усунення.

Внутрішньому аудиту СУІБ підлягають усі структурні підрозділи виконкому районної у місті ради.

Внутрішні аудити СУІБ складаються з постійних, періодичних (за графіком проведення внутрішніх аудитів) і позапланових перевірок.

Під час перевірки аудитори здійснюють:

1) оцінку:
- реалізації політики та цілей в сфері інформаційної безпеки;
- відповідності вимогам ідентифікованої інформаційної безпеки;
- рівня та повноти виконання завдань і обов'язків у сфері інформаційної безпеки, покладених на персонал;

2) перевірку:
- ведення та зберігання документації;
- знань посадовими особами нормативних документів щодо здійснення відповідних процедур;
- стану та використання технічних засобів.

Позапланові перевірки проводяться за рішенням голови районної в місті ради, його заступників, керуючого справами виконкому районної в місті ради у випадках, пов'язаних з порушенням установлених правил і процедур та напередодні проведення позапланового інспекційного контролю.

Обсяг робіт при проведенні перевірки визначає уповноважений з питань розробки та впровадження системи управління інформаційною безпекою у виконкомі районної в місті ради.

За підсумками періодичних і позапланових внутрішніх аудитів складається звіт за підписом керівника групи аудиту та подається для розгляду й затвердження уповноваженому з питань розробки та впровадження системи управління інформаційною безпекою у виконкомі районної в місті ради. Копії звітів передаються керівникам структурних підрозділів виконкому районної в місті ради, які підлягали аудиту. За результатами внутрішніх аудитів СУІБ розробляються заходи щодо усунення зауважень, виявлених під час перевірок, і проводяться коригувальні або запобіжні дії в залежності від встановлених зауважень. Виявлені відхилення та невідповідності мають бути усунені в найкоротший термін.

7. Перегляд системи управління інформаційною безпекою керівництвом

Аналіз СУІБ керівництвом проводиться відповідно до Процедури якості «Аналіз системи управління якістю з боку керівництва» із врахуванням вимог даного розділу. Результати аналізу враховуються при підготовці розпоряджень голови районної в місті ради, спрямованих на підвищення ефективності діяльності в сфері інформаційної безпеки.

Вхідними даними для перегляду СУІБ є:

- статус дій за результатами попередніх аналізів СУІБ з боку керівництва;
- зміни зовнішніх і внутрішніх аспектів, які мають відношення до СУІБ;
- зворотний зв’язок про стан інформаційної безпеки, включаючи: 1) невідповідності та коригувальні дії; 2) результати моніторингу та вимірювань; 3) результати аудиту; 4) результат досягнення цілей інформаційної безпеки;
- зворотний зв’язок від зацікавлених сторін;
- результати оцінки ризиків і статус виконання плану по обробці ризиків;
- можливості для постійного поліпшення.

Вихідні дані перегляду керівництвом повинні містити будь-які рішення та дії стосовно:

- удосконалення СУІБ;
- оновлення оцінки ризиків та плану їх оброблення;
- зміни процедур і заходів безпеки, що впливають на інформаційну безпеку (за необхідності), для адекватного реагування на внутрішні або зовнішні події, що можуть мати значний вплив на СУІБ, включаючи зміни у:
    - вимогах до основних процесів виконкому районної в місті ради;
    - вимогах безпеки;
    - процесах, які впливають на існуючі вимоги;
    - нормативних чи правових вимогах;
    - контрактних зобов’язаннях;
    - рівнях ризику та/або критеріях прийняття ризиків;
    - потребах у ресурсах;
    - удосконаленні вимірювання ефективності заходів безпеки.

Записи про аналізування СУІБ зберігаються у уповноваженого з питань розробки та впровадження системи управління інформаційною безпекою, і мають включати записи із вхідними даними (довідки, звіти, акти тощо), так і вихідними даними (рішення, програми, плани тощо).

8. Удосконалення системи управління інформаційною безпекою

8.1. Постійне вдосконалення

Виконком районної в місті ради постійно поліпшує результативність своєї діяльності, зокрема СУІБ, застосовуючи політику та визначаючи цілі в сфері інформаційної безпеки (п. 4.2.2.1), використовуючи результати внутрішніх аудитів (р. 6), аналіз даних про інформаційну безпеку на підставі записів

(п. 4.3.3), проводячи коригувальні та запобіжні дії (п. 8.2), а також аналіз СУІБ керівництвом (р. 7).

8.2. Процедури реагування на інциденти безпеки здійснення коригувальних і запобіжних дій

У виконкомі районної в місті ради здійснюється реагування на інциденти в сфері інформаційної безпеки відповідно до Методики виявлення та реєстрації інцидентів. Всі інциденти фіксуються та піддаються аналізу з метою виявлення причин їх виникнення. Про інциденти складаються звіти. Визначені шляхи повідомлення про інцидент та забезпечено порядок зворотного зв'язку.

Проведення коригувальних та запобіжних дій по відношенню до потенційних або виявлених причин невідповідностей виконується відповідно до Процедур «Порядок планування, здійснення та контролю результативності коригувальних дій» та «Порядок планування, здійснення та контролю результативності запобіжних дій». із врахуванням вимог даного розділу Настанови.

При появі невідповідності у виконкомі проводиться:

- реагування на невідповідності, і залежно від обставин: 1) вживаються заходи щодо його виправлення; 2) опрацьовування наслідків;
- оцінка необхідності прийняття дій для усунення причин невідповідності з метою запобігання його повторення або появи в іншому місці, і для цього: 1) вивчається невідповідність; 2) визначається при-чина невідповідності; 3) визначається, чи існують подібні невідповідності або потенційні можливості їх виникнення;
- реалізація коригувальні дії;
- аналізування результативності виконаних коригувальних дій;
- при необхідності, вносяться зміни в СУІБ.

Коригувальні дії розробляються для усунення причин невідповідностей, виявлених під час проведення:

- планових чи позачергових зовнішніх перевірок (аудитів);
- планових чи позачергових внутрішніх аудитів;
- надходження рекламацій (зауважень) замовника;
- у разі невиконання встановлених вимог до процедур виконання робіт.

Коригувальні дії повинні здійснюватися негайно та ефективно в усіх випадках, коли виявляється невідповідність, пов'язана з адміністративними послугами виконкому районної в місті ради, матеріалами, що використовуються, та обладнанням або функціонуванням СУІБ виконкому.

Запобіжні дії виконуються у відношенні причин невідповідностей, які можуть виникнути. Необхідно проводити вивчення доступної інформації для виявлення, аналізу та усунення потенційних причин невідповідностей. Керівники структурних підрозділів виконкому районної в місті ради повинні постійно аналізувати свою діяльність та планувати запобіжні дії.

У загальному випадку запобіжні дії розробляються і застосовуються у випадках виявлення потенційних невідповідностей у ході критичного аналізування:

- діяльності виконкому;
- використання ресурсів (персонал, інфраструктура, екологічні умови);
- задоволеності замовника;
- записів.

Персоналу виконкому районної в місті ради рекомендовано визначати галузі, у яких можуть виникнути потенційні невідповідності, та повідомляти про це керівників.

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

Додаток
до Настанови з інформаційної безпеки виконкому Довгинцівської районної в місті ради

Рекомендований перелік документації системи управління інформаційною безпекою

Адміністративні документи СУІБ

Наказ про призначення представника вищого керівництва в СУІБ
Положення про службу безпеки
Положення про службу інформаційної безпеки
Посадова інструкція представника вищого керівництва по СУІБ
Посадова інструкція системного адміністратора
Наказ вищого керівництва про впровадження і підтримку СУІБ

Документи верхнього рівня

Настанова з інформаційної безпеки
Структура підпорядкованості в СУІБ
Структура процесів СУІБ
Політика СУІБ (зовнішня)
Політика СУІБ (внутрішня)
Цілі СУІБ по процесах
План обробки ризиків
Плани забезпечення безперервності діяльності
Положення про застосування напрямків інформаційної безпеки
Методика оцінки ризиків
Критерії прийняття ризиків
Аналіз досягнення цілей
Звіт про оцінку ризиків
Заява вищого керівництва про прийняття залишкових ризиків
Склад групи внутрішнього аудиту
Програма внутрішніх аудитів СКІБ
План внутрішнього аудиту СКІБ
Звіт про аудит СКІБ
План коригувальних та запобіжних дій в СКІБ
Аналіз СКІБ з боку вищого керівництва

Документи середнього (технічного) рівня

А6. Організація захисту інформації
Журнали реєстрації подій в галузі інформаційної безпеки
Журнал реєстрації дій з інформаційною безпекою третіх осіб

А.7. Менеджмент активів
Правила для прийнятного використання інформації та активів
Керівні вказівки по класифікації інформації
Реєстр інформаційних активів (класифікація ІА, відповідальність за ІА, маркування ІА, оцінка ІА)

А8. Управління персоналом
Процедура управління персоналом
Програми навчання персоналу щодо інформаційної безпеки
Заходи підвищення обізнаності
Правила інформаційної безпеки для конкретної посади
Угода про дотримання правил інформаційної безпеки
Угода про конфіденційність
Записи про навчання (атестацію)

А9. Фізична безпека
Процедура фізичного захисту організації
Схема периметра безпеки
Схема розташування будівель, приміщень
Схема розташування засобів обробки інформації
Паспорти зон особливої безпеки

А10. Управління комп'ютерами та мережами
Правила обслуговування засобів обробки інформації
Процедура менеджменту надання послуг третьою стороною
Процедура управління змінами в засобах обробки інформації
Процедура менеджменту продуктивності
Процедура антивірусного захисту
Процедура захисту цілісності програмного забезпечення та інформації
Процедура резервного копіювання
Процедура мережевого захисту
Процедура роботи з носіями інформації
Процедура обміну інформацією
Керівництва з обслуговування засобів обробки інформації
Процедура постійного контролю діяльності по обробці інформації
Журнал реєстрації дій користувачів
Журнали реєстрації дій адміністраторів

A11. Управління доступом
Процедура доступу до приміщень
Процедура доступу до персоналу
Процедура доступу до паперових архівів
Процедура доступу до засобів обробки інформації та інформаційних активів за межами підприємства
Процедура доступу до електронних архівів
Процедура доступу до засобів обробки інформації
Процедура доступу до програмного забезпечення
Процедура доступу до інформаційних систем
Процедура доступу до операційних систем
Процедура доступу до мереж
Правила парольного захисту
Правила чистого столу і екрану
Журнал реєстрації доступів
Аналіз зареєстрованих доступів

A12. Придбання, розробка та підтримка інформаційних систем
Процедура прийняття нового засобу обробки інформації, програмного забезпечення, інформаційної системи, мережі
Процедура розробки (доопрацювання) програмного забезпечення, інформаційної системи
Правила введення даних в засоби обробки інформації, програмне забезпечення, інформаційні системи
Процедура установки програмного забезпечення
Процедура доступу до вихідного коду програм

A13. Управління інцидентами
Процедура виявлення та реєстрації інцидентів
Журнал реєстрації інцидентів ІБ
Журнал реєстрації скарг і пропозицій ІБ

A14. Управління безперервністю робочих процесів
Процедура управління безперервністю робочих процесів
Плани відновлення робочих процесів
Записи про тестування планів відновлення

A15. Управління відповідністю вимогам
Процедура захисту персональних даних
Порядок здійснення оцінки технічної відповідності
Перечень застосовного законодавства
Перелік законодавчих і контрактових вимог по наявності та зберігання записів

Документи нижнього рівня

Пам’ятка з антивірусного захисту
Пам’ятка з резервного копіювання
Пам’ятка по роботі з паролями
Пам’ятка при роботі на персональному комп’ютері
Пам’ятка щодо обміну інформацією
Пам’ятка щодо введення інформації в інформаційні системи
Пам’ятка по роботі з електронними документами
Пам’ятка по роботі з паперовими документами
Порядок дій у разі нестандартної ситуації
Порядок дій у разі катастрофи
Пам’ятка щодо захисту персональних даних
Покажчики на входах в зони особливого захисту