*ЗАТВЕРДЖЕНО*

*Розпорядження міського голови*

 *02.03.2015 №75-р*

***НАСТАНОВА***

 ***з інформаційної безпеки виконкому Криворізької міської ради***

***1. Вступ***

Виконавчий комітет Криворізької міської ради є виконавчим органом міської ради, який утворюється нею на строк її повноважень, підзвітний і під-контрольний їй, а з питань здійснення ним делегованих повноважень органів виконавчої влади – підконтрольний відповідним органам виконавчої влади.

Повноваження виконкому міської ради закріплені Законом України «Про місцеве самоврядування в Україні» та рішенням міської ради від 27.11.2013 №2293 «Про розмежування повноважень між виконавчим комітетом, відді-лами, управліннями, іншими виконавчими органами міської ради та міським головою», зі змінами.

Утворені міською радою відділи та управління, інші виконавчі органи мі-ської ради підпорядковані виконкому та міському голові, підзвітні та підконт-рольні міській раді. Керівники та посадові особи відділів, управлінь, інших ви-конавчих органів міської ради призначаються на посаду та звільняються з неї міським головою одноособово. Окремі управління та відділи мають свої печат-ки із зображенням Державного герба України та своїм найменуванням, штампи та інші реквізити юридичної особи.

Відділи, управління, інші виконавчі органи міської ради в діяльності керуються Конституцією та законами України, указами Президента України, постановами Верховної Ради України та Кабінету Міністрів України, рішен-нями міської ради, її виконавчого комітету, розпорядженнями міського голови, Регламентом виконавчого комітету Криворізької міської ради, затвердженим рішенням виконкому міської ради від 14.08.2013 №285 «Про затвердження Регламенту виконавчого комітету Криворізької міської ради», зі змінами, (надалі – Регламент виконкому міської ради), іншими нормативно-правовими актами в межах делегованих повноважень, а також положеннями про відділи, управління, інші виконавчі органи міської ради.

Основні завдання виконкому визначені відповідно до повноважень ви-

конавчих органів сільських, селищних, міських рад, викладених у стст. 27 – 40 гл. 2 Закону України «Про місцеве самоврядування в Україні».

Контактна інформація:

адреса: 50101, Україна, м. Кривий Ріг, пл. Радянська, 1;

факс: 74-17-00;

е-mail: mvk99@ukrpost.ua

***2. Сфера застосування***

Система управління інформацію безпекою виконкому Криворізької міської ради впроваджена відповідно до вимог ДСТУ ISO/IEC 27001:2010.

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.

Система управління інформаційною безпекою виконкому міської ради як вхідні дані бере вимоги захисту інформації й очікування зацікавлених сторін та засобом необхідних дій і процесів видає результати захисту інформації, що задовольняють цим вимогам і очікуванням.

Дія системи управління інформаційною безпекою розповсюджується на всі відділи, управління, інші виконавчі органи міської ради.

***3. Нормативні посилання***

Настанова з інформаційної безпеки виконкому міської ради містить поси-лання на такі нормативні документи:

1. ДСТУ ISO/IEC 27001:2010 «Інформаційні технології. Методи та засоби досягнення інформаційної безпеки. Системи управління інформаційною безпе-кою. Вимоги (ISO/IEC 27001:2005, IDT)»;
2. Закон України «Про місцеве самоврядування в Україні»;
3. Закон України «Про захист персональних даних»;
4. Закон України «Про інформацію»;
5. Закон України «Про доступ до публічної інформації»;
6. Постанова Кабінету Міністрів України від 30 листопада 2011 року №1242 «Про затвердження Типової інструкції з діловодства у центральних ор-ганах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади»;
7. рішення міської ради від 27.11.2013 №2293 «Про розмежування повно-важень між виконавчим комітетом, відділами, управліннями, іншими вико-навчими органами міської ради та міським головою», зі змінами;
8. рішення виконкому міської ради від:
9. 08.02.2012 №71 «Про затвердження Інструкції з діловодства в органах місцевого самоврядування міста»;
10. 14.08.2013 №285 «Про затвердження Регламенту виконавчого комітету Криворізької міської ради», зі змінами;
11. 14.05.2014 №141 «Про затвердження Порядку обробки персональних даних, володільцем яких є Криворізька міська рада, її виконком», зі змінами;
12. розпорядження міського голови від:
13. 31.05.2011 №122-р «Про захист персональних даних», зі змінами;
14. 06.11.2013 №247-р «Про затвердження Процедур систем управління якістю та інформаційною безпекою у відділах, управліннях, інших виконавчих органах міської ради, виконкомах районних у місті рад», зі змінами;
15. 31.12.2014 №294-р «Про затвердження розподілу обов’язків між сек-ретарем міської ради, заступниками міського голови та керуючою справами виконкому міської ради».

***4. Система управління інформаційною безпекою***

***4.1. Основні положення***

Для функціонування системи управління інформаційною безпекою вста-новлено такі групи процесів (видів діяльності), що використовуються на всіх рівнях діяльності виконкому міської ради:

- процеси управління 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, що засто-совується для структуризації всіх процесів системи управління інформаційною безпекою.

Процеси характеризуються наявністю:

1. постачальника процесу;
2. власника процесу;
3. споживача процесу;
4. вхідних та вихідних даних процесу;
5. ресурсів, необхідних для виконання процесу;
6. критеріїв моніторингу і контролю процесу;
7. відповідальних за виконання процесу.

Задокументована система управління інформаційною безпекою виконко-му Криворізької міської ради є доступною, її вимоги обов’язкові для персоналу відділів, управлінь, інших виконавчих органів міської ради. У свою чергу персонал виконкому повинен забезпечувати ефективне виконання документо-ваних процедур та інструкцій системи управління інформаційною безпекою.

***4.2. Менеджмент системи управління інформаційною безпекою***

***4.2.1. Планування системи управління інформаційною безпекою***

***4.2.1.1. Політика у сфері інформаційної безпеки виконкому міської ради***

Політика у сфері інформаційної безпеки виконкому міської ради (надалі – Політикау сфері інформаційної безпеки) затверджується розпорядженням міського голови. Вона розробляється відповідно до вимог чинного законо-давства України, ДСТУ ISO/IEC 27001:2010. Політика визначає місію, пріоритети та принципи діяльності виконкому міської ради в сфері інфор-маційної безпеки й основні шляхи їх реалізації.

Працівники відділів, управлінь, інших виконавчих органів міської ради мають володіти положеннями Політики у сфері інформаційної безпеки та забез-печувати її реалізацію.

Пропозиції щодо внесення змін і доповнень до Політики у сфері інфор-маційної безпеки подаються посадовою особою відділу, управління, іншого виконавчого органу міської ради, відповідальною за функціонування системи управління інформаційною безпекою, на розгляд головному уповноваженому з питань управління якістю та інформаційною безпекою виконкому міської ради. Політика у сфері інформаційної безпеки переглядається за потреби, але не рідше 1 разу на рік.

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

***4.2.1.2. Оцінка ризиків***

Виявлення й оцінка ризиків інформаційної безпеки відбувається відповід-но до Методики управління ризиками. Основними завданнями Методики управління ризиками є:

 - установлення ефективної системи підтримки прийняття управлінських

рішень з урахуванням рівня ризиків у сфері інформаційної безпеки;

1. забезпечення здійснення діяльності виконкому міської ради у відповід-ності до встановлених політик, процедур і регламентів;
2. 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. Форма документування регламентована методикою управління ризиками інформацій-ної безпеки. Погоджені ризики вважаються прийнятими.

Ризики інформаційної безпеки, що прийняті, але за ними не плануються заходи безпеки (залишкові ризики) погоджуються керівництвом окремо з об-ґрунтуванням 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 фун-кціональних обов’язків і процесів, обсяг можливих збитків.

Методологія оцінки ризиків може бути кількісною, якісною або ком-бінованою.

Перегляд оцінки ризиків відбувається за потребою або в разі виникнення інциденту у сфері інформаційної безпеки, упровадження нових чи вилучення існуючих процесів.

***4.2.1.3. Положення про застосовність цілей***

***заходів інформаційної безпеки***

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

***4.2.2. Упровадження заходів безпеки, процесів та***

***процедур системи управління інформаційною безпекою***

***4.2.2.1. Планування оброблення ризиків***

Вхідними даними для планування оброблення ризиків є:

1. законодавчі та нормативні вимоги;
2. Політика у сфері інформаційної безпеки;
3. цілі управління інформаційною безпекою;
4. рішення щодо залишкових ризиків;
5. аналіз даних нагляду за виконанням процесів системи управління інфор-маційною безпекою;
6. інформація щодо ресурсів (персоналу, інфраструктури, виробничого се-редовища, матеріалів, технічних засобів тощо);
7. виявлені можливості для вдосконалення.

Вихідними даними планування оброблення ризиків є рішення щодо:

1. розробки правил та політики управління інформацією, зокрема доку-ментами;
2. здійснення заходів з обробки ризиків, зокрема щодо зменшення або уни-кнення ризиків інформаційної безпеки;
3. розподілу повноважень і відповідальності;
4. розвитку інфраструктури та ресурсної бази;
5. забезпечення виконкому міської ради компетентним персоналом.

Перегляд планів упровадження заходів безпеки відбувається за потреби, або в разі виникнення інциденту інформаційної безпеки, вилучення або впровадження нових процесів.

Аналіз ефективності заходів безпеки у відділах, управліннях, інших виконавчих органах міської ради здійснює посадова особа, відповідальна за функціонування системи управління інформаційною безпекою.

***4.2.2.2. Процеси інформування***

Міський голова та керівники відділів, управлінь, інших виконавчих орга-нів міської ради встановлюють і забезпечують наявність результативних про-цесів обміну інформацією, пов’язаною з діяльністю виконкому міської ради та результативністю системи управління інформаційною безпекою. Вимоги до об-міну інформацією встановлено Регламентом виконкому міської ради.

У виконкомі міської ради використовуються такі методи внутрішнього та зовнішнього інформування:

1. розміщення інформації на стендах;
2. представлення інформації на нарадах у керівництва чи зборах колективу;
3. розповсюдження інформації в локальній комп’ютерній мережі, через офіційні веб-сайти виконкому міської ради та районних у місті рад у мережі Інтернет та електронні інформаційні ресурси міста на порталі «Криворізький ресурсний центр»;
4. розповсюдження копій документів на паперових та електронних носіях;
5. видача наказів та розпоряджень керівництва;
6. засоби масової інформації.

Керівники відділів, управлінь, інших виконавчих органів міської ради в межах своїх повноважень несуть відповідальність за додержання персоналом професійної таємниці щодо інформації, яку вони отримують у результаті вико-нання роботи від суб’єктів господарювання, громадян.

Загальні вимоги до забезпечення конфіденційності доводяться до всього персоналу виконкому міської ради. Усі документи та інформація, що надійшли від громадян, юридичних і фізичних осіб-підприємців, не можуть передава-тися третій особі без їх письмової згоди.

Виконком міської ради несе відповідальність за належне збереження влас-ності замовника відповідно до чинного законодавства України, повинен дбати про будь-яку інформацію, документи, матеріали чи інші предмети, надані за-мовниками послуг для опрацювання (послуга, процес, перевірка, затвердження тощо).

***4.2.3. Процедура моніторингу та контролю***

У виконкомі міської ради здійснюється контроль за діями персоналу, ро-ботою програмного забезпечення тощо. Оперативний контроль виконавчої дис-ципліни, дотримання встановлених процедур та внутрішній аудит системи уп-равління інформаційною безпекою здійснюються відповідно до вимог чинного законодавства України. Вимоги до методів здійснення контролю викладені в Регламенті виконавчого комітету Криворізької міської ради, Настанові з інфор-маційної безпеки, розпорядженнях міського голови. Вимоги спрямовані на ви-явлення та термінове реагування на інциденти інформаційної безпеки, помилки в результаті обробки інформації, підвищення продуктивності діяльності щодо гарантування інформаційної безпеки, подій безпеки, оцінку ефективності дій з усунення порушень безпеки.

***4.2.4. Перегляд ефективності системи***

***управління інформаційною безпекою***

Для здійснення перегляду ефективності системи управління інформа-ційною безпекою виконкомом міської ради впроваджені та підтримуються процеси моніторингу, вимірювань, аналізу й поліпшення інформаційної безпеки.

Вони спрямовані на:

1. створення відкритих, зручних і доступних умов для отримання якісних публічних послуг мешканцями міста;
2. забезпечення відповідності системи управління інформаційною безпе-кою виконкому міської ради вимогам ДСТУ ISO/IEC 27001:2010;
3. постійне поліпшення функціонування системи управління інформацій-ною безпекою.

Ці процеси полягають в одержанні, обробці та узагальненні інформації про функціонування системи управління інформаційною безпекою, її 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 ефективного функціонування та розвитку системи управління інформаційною безпекою у виконкомі міської ради розроблено та впроваджено нормативну документацію системи інформаційної безпеки:

1. Політику в сфері інформаційної безпеки;
2. Настанову з інформаційної безпеки виконкому Криворізької міської ра-ди;
3. Положення про застосовність цілей заходів інформаційної безпеки;
4. реєстр інформаційних активів;
5. перелік можливих ризиків інформаційної безпеки та план їх обробки;
6. методику управління інцидентами інформаційної безпеки;
7. процедури та протоколи, що підтверджують реалізацію функцій і вимог системи управління інформаційною безпекою;
8. інші документи, на які є посилання в процедурах та інструкціях.

Настанова з інформаційної безпеки виконкому Криворізької міської ради (надалі – Настанова) – це опис функціонування системи управління інформа-ційною безпекою у виконкомі міської ради, який є його власністю. Вона вста-новлює цілі, задачі та принципи функціонування системи управління інформаційною безпекою, розподіл повноважень і відповідальності серед керівників та працівників відділів, управлінь, інших виконавчих органів міської ради на всіх етапах виконання управлінських і контрольних функцій.

Настанова призначена для використання в цілях:

1. забезпечення стабільного функціонування системи управління інформа-ційною безпекою, її самооцінки та вдосконалення;
2. підготовки персоналу для виконання робіт відповідно до вимог системи управління інформаційною безпекою;
3. забезпечення необхідної інформації при проведенні перевірок системи управління інформаційною безпекою;
4. інформування зацікавлених сторін (громадян, юридичних, фізичних осіб-підприємців) про Політику та процедури виконкому міської ради в сфері інформаційної безпеки.

Настанова розповсюджується на всі процеси, пов’язані з інформаційною безпекою, та встановлює вимоги до функціонування системи управління нею.

У Настанові застосовуються терміни та визначення, установлені ДСТУ ISO/IEC 27001:2010.

Положення Настанови 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 не обмежений, її зміст переглядається та вдоско-налюється за потреби, але не рідше 1 разу на рік.

У разі, якщо на думку будь-якого співробітника окремі положення Наста-нови або вона в цілому не відповідають у повній мірі вимогам забезпечення належного рівня функціонування системи управління інформаційною безпекою, він має право звернутися до головного уповноваженого з питань систем управління якістю та інформаційною безпекою або посадової особи, відповідальної за функціонування системи управління інформаційною безпекою, з пропозицією про проведення її коригування.

Рішення про перегляд та коригування Настанови приймає головний уповноважений з питань систем управління якістю та інформаційною безпекою.

Документація системи управління інформаційною безпекою, зберігається у відділах, управліннях, інших виконавчих органах міської ради та використо-вується персоналом для ефективного виконання встановлених вимог.

***4.3.2. Контроль документів***

Виконком міської ради здійснює управління документацією на підставі Регламенту виконкому міської ради, який визначає принципи та порядок:

 – організації:

 - роботи зі службовими документами;

 - контролю за виконанням нормативно-правових актів законодавчої й виконавчої влади, актів міської ради, її виконавчого комітету та міського голови;

 - використання фірмових бланків, гербових печаток, печаток без зображення герба, штампів;

– забезпечення:

 - наявності відповідних версій чинних документів у місцях застосування;

 - ідентифікації змін та статусу чинної версії документів;

 - контролю за розповсюдженням документів;

 – роботи:

 - зі скаргами, заявами, зверненнями, пропозиціями та інформа-ційними запитами;

 - з єдиним електронним реєстром документів виконкому;

 - у локальній комп’ютерній мережі виконкому міської ради та з електронною поштою;

 – запобігання ненавмисному застосуванню застарілих документів;

 – розміщення матеріалів на офіційному веб-сайті виконкому Криворізь-кої міської ради в мережі Інтернет;

 – формування справ у діловодстві виконкому міської ради, тимчасово-го зберігання та використання архівних документів;

 – взаємодії із засобами масової інформації та громадськістю.

Вимоги до документації системи управління інформаційною безпекою викладені в Інструкції з діловодства в органах місцевого самоврядування міста, затвердженій рішенням виконкому міської ради від 08.02.2012 №71.

***4.3.3. Контроль записів***

Для результативної реалізації функцій і вимог системи управління ін-формаційною безпекою виконкомом міської ради впроваджуються та ведуться протоколи, що фіксують факт події в сфері інформаційної безпеки або її результати. Порядок поводження з протоколами викладено в Регламенті виконкому міської ради, Інструкції з діловодства в органах місцевого само-врядування міста.

Управління протоколами здійснюється на етапах:

1. розробки форми;
2. упровадження протоколу;
3. унесення даних;
4. зберігання протоколу.

***5. Відповідальність керівництва***

***5.1. Зобов’язання керівництва***

З метою забезпечення належного контролю за функціонуванням систем управління якістю та інформаційною безпекою розпорядженням міського голови від 31.12.2014 №294-р «Про затвердження розподілу обов’язків між секретарем міської ради, заступниками міського голови та керуючою справами виконкому міської ради» головним уповноваженим з питань систем управління якістю та інформаційною безпекою виконкому міської ради (надалі – голов-ний уповноважений) визначено заступника міського голови Подоплєлову Н.Л., на яку покладено повноваження з координації та контролю за роботою з питань функціонування систем управління якістю органів місцевого само-врядування міста та інформаційною безпекою виконкому міської ради. У кожному відділі, управлінні, іншому виконавчому органі міської ради призначено посадових осіб, відповідальних за забезпечення функціонування систем управління інформаційною безпекою, 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, аналіз, підтримку в робочому стані та поліпшення системи управління інформаційною безпекою;

- гарантування направленості процедур захисту інформації на виконання вимог чинного законодавства України в сфері інформаційної безпеки, стандар-ту ISO/IEC 27001:2010;

- виявлення та розгляд нормативних і законодавчих вимог, договірних зо-бов’язань щодо захисту інформаційних активів;

- проведення аналізу функціонування системи управління інформаційною безпекою та реагування на його результати;

- поліпшення результативності системи управління інформаційною без-пекою.

До ресурсів належать:

1. персонал виконкому міської ради;
2. інфраструктура;
3. фінанси.

Планування ресурсів здійснюється в рамках планування діяльності, роз-витку та матеріально-технічного забезпечення виконкому міської ради.

При цьому вирішуються питання:

1. планування потреб у ресурсах;
2. забезпечення необхідними матеріальними та нематеріальними (інтелек-туальними) ресурсами;
3. забезпечення персоналом, підтримка та підвищення його кваліфікації;
4. розвиток інфраструктури.

***5.2.2. Навчання, поінформованість та компетентність***

Реалізація проголошеної Політики в сфері інформаційної безпеки та до-сягнення поставлених завдань розвитку здійснюються через:

1. визначення вимог до компетентності посадових осіб (персоналу викон-кому – посадових осіб, спеціалістів та робітників), їх обов’язків і повно-важень;
2. забезпечення професійної підготовки та постійної підтримки кваліфіка-ції посадових осіб;
3. доведення до працівників поставлених завдань, оперативної інформації та значимості їх діяльності в галузі захисту інформації, їх вкладу в досягнення цілей системи управління інформаційною безпекою;
4. оцінку результативності дій (навчання, інформування).

Підвищення кваліфікації працівників виконкому здійснюється через нав-чання у відповідних навчальних закладах раз на 5 років та шляхом:

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

Уся інформація про професійну підготовку спеціалістів, набутий досвід роботи та види навчання містяться в персональних справах співробітників, що зберігаються в кадровій службі виконкому міської ради.

***6. Внутрішній аудит системи***

***управління інформаційною безпекою***

Порядок проведення внутрішніх аудитів системи управління інформацій-ною безпекою регламентовано Процедурою якості «Порядок проведення внут-рішніх аудитів».

Метою внутрішнього аудиту є здійснення моніторингу, забезпечення дот-римання базових принципів гарантування інформаційної безпеки виконкому міської ради, її відповідності вимогам нормативних документів, своєчасне виявлення відхилень, недоліків і розробка заходів щодо їх усунення.

Внутрішніми перевірками охоплюються всі відділи, управління, інші ви-конавчі органи міської ради. Можуть проводитися скомбіновані внутрішні аудити (одночасно аудити систем управління якістю та інформаційною безпекою).

Внутрішні аудити складаються з планових (за графіком) і позапланових перевірок.

Під час перевірки аудитори здійснюють:

– оцінку:

 - реалізації Політики та цілей в сфері інформаційної безпеки;

 - відповідності інформаційних активів виконкому міської ради вимо-гам ідентифікованої інформаційної безпеки;

 - рівня та повноти виконання завдань і обов’язків у сфері інформа-ційної безпеки, покладених на персонал;

– перевірку:

 - ведення та зберігання документації;

 - знання посадовими особами нормативних документів щодо здійснен-ня відповідних процедур;

 - стану та використання технічних засобів.

Позапланові перевірки проводяться за рішенням міського голови, його за-ступників, керуючої справами виконкому міської ради або керівників відділів, управлінь, інших виконавчих органів міської ради у випадках, пов’язаних з по-рушенням установлених правил і процедур, або напередодні проведення позапланового інспекційного контролю.

Обсяг робіт при проведенні перевірки визначає головний уповноважений з питань систем управління якістю та інформаційною безпекою виконкому міської ради.

За підсумками внутрішніх аудитів складається звіт за підписом керівника групи з аудиту та подається для розгляду головному уповноваженому з питань систем управління якістю та інформаційною безпекою виконкому міської ради.

 Копії звітів передаються керівникам відділів, управлінь, інших виконавчих органів міської ради, що підлягали аудиту. За результатами внутрішніх аудитів розробляються заходи щодо усунення зауважень, виявлених під час перевірок, і проводяться коригувальні або запобіжні дії в залежності від установлених порушень. Виявлені відхилення та невідповідності мають бути усунені в най-коротший термін.

***7. Перегляд системи управління***

***інформаційною безпекою керівництвом***

Аналіз системи управління інформаційною безпекою керівництвом про-водиться відповідно до Процедури якості «Аналіз системи управління якістю з боку керівництва». Результати аналізу враховуються при підготовці оператив-них розпоряджень, спрямованих на підвищення ефективності діяльності в сфері інформаційної безпеки.

Вхідними даними для перегляду системи управління інформаційною без-пекою є:

- результати аудитів та переглядів системи управління інформаційною безпекою;

- зворотний зв’язок із зацікавленими сторонами;

- методи, продукти або процедури вдосконалення продуктивності та ефе-ктивності системи управління інформаційною безпекою;

- статус запобіжних та коригувальних дій;

- вразливості або загрози, що не були адекватно враховані в попередній оцінці ризиків;

- результати вимірів ефективності системи управління інформаційною безпекою;

- дії, що є наслідком попереднього перегляду керівництвом;

- будь-які зміни, що можуть мати вплив на систему управління інформа-ційною безпекою;

- рекомендації щодо її вдосконалення.

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

- удосконалення ефективності системи управління інформаційною безпе-кою;

- оновлення оцінки ризиків та плану їх обробки;

- модифікації процедур і заходів безпеки, що впливають на інформаційну безпеку (за необхідності), для адекватного реагування на внутрішні або зов-нішні події, що можуть мати значний вплив на систему інформаційної безпеки, включаючи зміни в:

- вимогах до основних процесів виконкому міської 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.

***8. Удосконалення системи управління інформаційною безпекою***

***8.1. Постійне вдосконалення***

Виконком міської ради постійно поліпшує результативність своєї діяль-ності та систему управління інформаційною безпекою, застосовуючи Політику у сфері інформаційної безпеки, використовуючи результати внутрішніх аудитів, аналіз даних, проводячи коригувальні та запобіжні дії, а також аналіз системи управління інформаційною безпекою керівництвом.

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

У виконкомі міської ради здійснюється реагування на інциденти в сфері інформаційної безпеки. Всі інциденти фіксуються та піддаються аналізу з ме-тою виявлення причин їх виникнення. Про інциденти складаються звіти. Визначено шляхи повідомлення про інцидент та забезпечено порядок зво-ротного зв’язку.

Проведення коригувальних і запобіжних дій у відношенні до потенційних або виявлених причин невідповідностей виконується згідно з Процедурою якості «Порядок планування, здійснення та контролю ефективності коригу-вальних і запобіжних дій».

У загальному випадку коригувальні дії розробляються для усунення при-чин невідповідностей, виявлених під час проведення:

- планових чи позапланових зовнішніх перевірок (аудитів);

1. планових чи позапланових внутрішніх аудитів;
2. надходження рекламацій (зауважень) замовника послуг та в разі невиконання встановлених вимог до процедур виконання робіт.

При виявленні невідповідностей керівники відділів, управлінь, інших ви-конавчих органів міської ради здійснюють:

1. аналіз виявленої невідповідності з метою визначення причини її виник-нення;
2. визначення коригувальних дій, термінів і відповідальних за усунення причин невідповідностей;
3. оцінку потреби в заходах, які гарантують, що невідповідності не повто-ряться;
4. контроль за виконанням запланованих коригувальних дій;
5. документальну реєстрацію результатів виконаних коригувальних дій;
6. аналіз ефективності виконаних коригувальних дій.

Коригувальні дії мають здійснюватися негайно та ефективно в усіх ви-падках, коли виявляється невідповідність, пов’язана з послугами виконкому міської ради, матеріалами, що використовуються, та обладнанням або функціо-нуванням системи управління інформаційною безпекою виконкому.

Запобіжні дії виконуються відносно причин невідповідностей, що можуть виникнути. Потрібно проводити вивчення доступної інформації для виявлення, аналізу та усунення потенційних причин невідповідностей. Керівники відділів, управлінь, інших виконавчих органів міської ради повинні постійно аналізувати свою діяльність та планувати запобіжні дії. Персоналу виконкому міської ради рекомендовано визначати галузі, у яких можуть виникнути потенційні невідповідності, та повідомляти про це своїх безпосередніх керівників.

***Керуюча справами виконкому О.Шовгеля***