*Додаток*

*до розпорядження міського голови*

*23.01.2015 №22-р*

***Процедура систем управління***

***якістю, інформаційною безпекою***

***«Порядок проведення внутрішніх аудитів»***

***1. Загальні положення***

1. . Процедура систем управління якістю, інформаційною безпекою «По-рядок проведення внутрішніх аудитів» (надалі – процедура) розроблена з метою визначення єдиних підходів до організації та проведення внутрішніх аудитів, підготовки аудиторських звітів, висновків та рекомендацій у викон-комі міської ради відповідно до вимог ДСТУ ISO 19011:2012.
2. . Процедура визначає порядок моніторингу та удосконалення діяльності виконкому міської ради шляхом проведення внутрішніх аудитів на предмет функціонування систем управління якістю (СУЯ) та інформаційною безпекою (СУІБ) у виконкомі міської ради відповідно до вимог ДСТУ ISO 9001:2009

та ISO/ІЕС 27001:2010.

1. . Предметом процедури є дії членів групи аудиту й посадових осіб ви-конкому міської ради при плануванні, підготовці та проведенні внутрішнього аудиту СУЯ, СУІБ (надалі – внутрішній аудит). Об’єктами внутрішнього аудиту є відділи, управління, інші виконавчі органи міської ради.
2. . Внутрішні аудити проводяться за необхідності, але не рідше 1 разу на рік. Тривалість внутрішнього аудиту планується, виходячи з його обсягу й поставленої мети, складу групи аудиту, але за будь-яких обставин не може перевищувати 5 робочих днів.
3. . Внутрішній аудит може бути плановим і позаплановим. Позаплановий внутрішній аудит може проводитися у випадках:

1.5.1 істотних змін у організаційній структурі виконкому міської ради;

1.5.2 унесення значних змін до керівних документів з якості та інформа-ційної безпеки;

1.5.3 наявності незадоволеності споживачів або виявлених сторонніми ор-ганізаціями невідповідностей якості надання послуг установленим законом вимогам;

1.5.4 необхідності перевірки виконання запобіжних та коригувальних дій і їх результатів;

1.5.5 виявлення критичних невідповідностей у поточній діяльності.

1. . Процедура обов'язкова для виконання в повному обсязі всіма відділами, управліннями, іншими виконавчими органами міської ради в частині взаємодії з групою аудиту.

1.7. Дані про внутрішні аудити включаються до звіту про функціонування СУЯ та СУІБ за звітний період.

***2. Нормативні посилання***

У цій процедурі використані посилання на такі нормативні документи:

* ДСТУ ISO 9000:2007 «Система управління якістю. Основні положення та словник термінів»;
* ДСТУ ISO 9001:2009 «Система управління якістю. Вимоги»;
* ДСТУ ISO 19011:2012 «Настанови щодо здійснення аудитів систем уп-равління»;
* ДСТУ IWA 4:2009 «Системи управління якістю. Настанови щодо зас-тосовування ISO 9001:2008 в суб’єктах місцевого самоврядування»;
* ДСТУ ISO/ІЕС 27001:2010 «Інформаційні технології. Методи та засоби досягнення інформаційної безпеки. Системи керування інформаційною безпе-кою. Вимоги (ISO/ІЕС 27001:2005, ІDT)»;
* Настанова щодо якості виконкому Криворізької міської ради;
* Настанова з інформаційної безпеки виконкому Криворізької міської ради.

***3. Організація та підготовка внутрішнього аудиту***

3.1. Внутрішні аудити проводять підготовлені аудитори. Підготовкою аудиторів керує головний уповноважений з питань систем управління якістю та інформаційною безпекою виконкому міської ради – заступник міського голови (надалі – головний уповноважений).

3.2. Навчання аудиторів проводяться як уповноваженою сторонньою організацією, так і внутрішні. Уповноважена стороння організація проводить навчання аудиторів з видачею відповідного документа (сертифіката, свідоцтва тощо). Внутрішні навчання проводяться аудиторами виконкому міської ради, які мають документ про навчання, відповідно до затвердженого графіка, за визначеними темами. Інформація про підготовлених аудиторів заноситься до реєстру внутрішніх аудиторів виконкому міської ради (додаток 1).

3.3. Група аудиторів добирається відповідно до їх компетентності, практичного досвіду та незалежності аудитора від відділу, управління, іншого виконавчого органу міської ради, що підлягає перевірці (надалі – аудитованого підрозділу).

3.4. Програма внутрішніх аудитів та графік їх проведення складаються відділом дозвільно-погоджувальних процедур виконкому міської ради, затверджуються до 01 січня щорічно головним уповноваженим і розсилаються аудитованим підрозділам для врахування в роботі.

3.5. Формування програми внутрішніх аудитів здійснюється шляхом:

3.5.1 установлення цілей їх проведення;

3.5.2 визначення критеріїв та обсягу робіт;

3.5.3 оцінювання можливих ризиків та ресурсів для проведення;

3.5.4 визначення компетентності груп аудитів та їх керівників;

3.5.5 зазначення вимог до конфіденційності;

3.5.6 обрання методів проведення аудитів та документування їх результатів.

3.6. Графік проведення внутрішніх аудитів складається з урахуванням чинної структури виконкому міської ради, з урахуванням статусу та важ-ливості процесів, що підлягають перевірці, а також результатів попередніх перевірок. У графіку зазначається назва підрозділу, що підлягає перевірці та термін її проведення.

3.7. За місяць до визначеного терміну проведення внутрішнього аудиту призначається група аудиту, визначається її керівник. Керівник групи аудиту складає план його проведення, який погоджується з аудитованими під-розділами та головним уповноваженим і розміщується в локальній мережі виконкому міської ради.

3.8. При підготовці плану майбутнього аудиту може бути передбачена ви-біркова перевірка виконання коригувальних заходів відносно раніше вияв-лених невідповідностей та проведення вибіркового розгляду робочих до-кументів (методик, інструкцій, програм тощо), що стосуються питань якості, протидії корупційним загрозам, інформаційної безпеки й використовуються аудитованим підрозділом у діяльності, з метою включення в план тих питань, на яких слід сконцентрувати увагу при аудиті.

3.9. У плані внутрішнього аудиту зазначаються:

3.9.1 аудитовані підрозділи;

3.9.2 сфера, мета та задачі внутрішнього аудиту;

3.9.3 дата, час та тривалість його проведення;

3.9.4 склад групи аудиту, розподіл обов’язків між аудиторами та залученими до аудиту фахівцями (технічні експерти, стажисти, супроводжуючі особи);

3.9.5 критерії аудиту;

3.9.6 методи проведення та документування результатів аудиту;

3.9.7 розподіл ресурсів;

3.9.8 вимоги до конфіденційності.

3.10. Призначення групи аудиту.

3.10.1 Керівником групи аудиту призначається начальник відділу, уп-равління, іншого виконавчого органу міської ради, до повноважень якого віднесені питання координації роботи з питань функціонування та розвитку СУЯ та СУІБ в органах місцевого самоврядування ( у разі відсутності – його заступник). У разі перевірки цього структурного підрозділу, керівником групи призначається інший внутрішній аудитор відповідно до реєстру внутрішніх аудиторів виконкому міської ради з урахуванням його компетентності.

3.10.2 Кількісний склад групи аудиту визначається залежно від обсягу аудиту, його тривалості та може складати від 2 до 5 осіб, включаючи керівни-ка групи.

3.11. У перший день аудиту перед його початком (у разі необхідності) проводиться нарада, у якій беруть участь члени групи аудиту, керівництво й задіяні працівники аудитованого підрозділу. Нарада проводиться керівником групи аудиту.

3.12. Порядок денний наради може включати такі питання:

3.12.1 представлення членів групи аудиту із зазначенням ролі в його про-веденні;

3.12.2 обговорення програми, підтвердження цілей аудиту;

3.12.3 відносно порядку проведення аудиту;

3.12.4 призначення терміну й порядку підсумкової наради (у разі необ-хідності).

***4. Компетентність і оцінювання внутрішніх аудиторів***

4.1. Компетентність персоналу, залученого до проведення внутрішніх ауди-тів, базується на знаннях та вміннях, набутих завдяки освіті, практичній робо-ті, аудиторській підготовленості та досвіду проведення аудитів.

4.2. Керівник групи аудиту повинен мати повне розуміння процесу й здатність використовувати всі особисті риси та вміння, необхідні для забез-печення ефективного й результативного управління та лідерства в процесі аудиту.

4.3. Керівником групи може бути призначена особа, яка брала участь у про-цесах не менше 3 завершених аудитів і виконувала функції керівника групи аудиту під наглядом та керівництвом іншого керівника групи щонайменше в одному з цих 3 аудитів.

4.4. Вимоги до внутрішніх аудиторів щодо:

4.4.1. Кваліфікації (знань):

4.4.1.1 володіння вимогами основних документів, у тому числі ДСТУ ISO 9001:2009 та ISO/ІЕС 27001:2010, документації СУЯ та СУІБ виконкому місь-кої ради;

4.4.1.2 знання засад, методів і організації перевірки СУЯ та СУІБ відпо-відно до ДСТУ ISO 19011:2012 «Настанови щодо здійснення аудитів систем управління»;

4.4.1.3 офіційна підготовка з питань функціонування СУЯ та СУІБ, під-тверджена свідоцтвом про складання іспитів чи про присвоєння відповідної професійної кваліфікації, виданим акредитованим органом (хоча б одного з членів групи аудиту).

4.4.2. Досвіду:

4.4.2.1 робота у виконкомі міської ради не менше 3 років;

4.4.2.2 участь щонайменше у повних процесах 2 внутрішніх аудитів під наглядом і керівництвом аудитора.

4.4.3. Особистих рис:

4.4.3.1 етичність;

4.4.3.2 неупередженість;

4.4.3.3 дипломатичність;

4.4.3.4 об'єктивність;

4.4.3.5 наполегливість;

4.4.3.6 уміння аналітично та гнучко мислити, діяти відповідально й неза-лежно приймати рішення;

4.4.3.7 цілеспрямованість у поліпшенні дії СУЯ та СУІБ виконкому міської ради;

4.4.3.8 нерозголошення конфіденційної інформації, отриманої в ході про-ведення внутрішніх аудитів.

4.5. Знання та вміння, пов’язані з керуванням інформаційною безпекою та застосуванням спеціалізованих методів, способів, процесів і практики мають бути достатніми, щоб аудитор міг фахово перевіряти систему управління, формувати належні дані та висновки аудиту, володіти:

4.5.1 основними положеннями законів і регламентів у сфері інформаційної безпеки;

4.5.2 принципами керування ризиками інформаційної безпеки;

4.5.3 методами й практиками цілісності та конфіденційності інформації тощо.

4.6. Проведення оцінювання внутрішніх аудиторів на відповідність уста-новленим вимогам здійснюється в ході співбесіди з головним уповноваженим та шляхом аналізу результатів їх попередніх аудитів (за наявності).

4.7. Після призначення групи аудиту необхідно передбачити час на її підготовку. Обов’язком керівника групи є організація й проведення підго-товки групи, що включає:

4.7.1. ознайомлення групи аудиту з його обсягом і тематикою;

4.7.2. збір повної інформації про аудитований підрозділ;

4.7.3. обговорення програми аудиту, розподіл робіт між членами групи аудиту, зокрема визначення робочих приміщень і конкретних дій кожного аудитора.

***5. Відповідальність і повноваження***

5.1. Ця процедура встановлює повноваження й відповідальність головного уповноваженого, відділу, управління, іншого виконавчого органу міської ради, до повноважень якого віднесені питання координації роботи з питань функціонування та розвитку СУЯ та СУІБ в органах місцевого само-врядування, керівника аудитованого підрозділу, керівника групи аудиту й аудиторів при проведенні внутрішніх аудитів.

5.2. Головний уповноважений:

5.2.1. Затверджує програми, графіки внутрішніх аудитів та погоджує плани їх проведення, аналізує звіти про підсумки проведення.

5.2.2. Забезпечує вжиття заходів щодо запобігання неправомірному втру-чанню третіх осіб у планування та проведення внутрішнього аудиту, під-готовку звіту про його результати.

5.2.3. Приймає рішення про проведення позапланових аудитів із вказівкою мети та обсягу.

5.2.4. Ухвалює рішення з усіх спірних питань, що виникають між групою аудиту та аудитованим підрозділом.

5.2.5. Погоджує питання про залучення в групу аудиту необхідних фахівців відділів, управлінь, інших виконавчих органів міської ради, залежно від тематики аудиту (технічних експертів, стажистів тощо).

5.2.6. Визначає та оцінює можливі ризики, пов’язані з програмою аудитів.

5.2.7. Планує ресурси для здійснення процесів внутрішніх аудитів систем управління.

5.2.8. Приймає рішення про оприлюднення звітів за результатами внут-рішніх аудитів.

5.3. Відділ, управління, інший виконавчий орган міської ради, до повно-важень якого віднесені питання координації роботи з питань функціонування та розвитку СУЯ і СУІБ в органах місцевого самоврядування:

5.3.1. Розробляє та подає на затвердження головному уповноваженому програми, графіки внутрішніх аудитів, опитувальні анкети.

5.3.2. Готує й відправляє повідомлення про проведення внутрішніх аудитів аудитованим підрозділам.

5.3.3. Здійснює методичне керівництво з питань проведення внутрішніх аудитів у відділах, управліннях, інших виконавчих органах міської ради;

5.3.4. Організовує навчання внутрішніх аудиторів.

5.3.5. Контролює виконання запобіжних та коригувальних заходів, розроблених аудитованим підрозділом за наслідками аудиту.

5.3.6. Взаємодіє з аудитованими підрозділами до повного усунення всіх невідповідностей, виявлених під час проведення внутрішніх аудитів та зазначених у звіті.

5.4. Керівник групи аудиту:

5.4.1. Визначає склад групи аудиту, розподіляє завдання та обсяги роботи між членами групи та, за потреби, коригує їх.

5.4.2. Уносить пропозиції головному уповноваженому про залучення до внутрішнього аудиту необхідних фахівців (технічних експертів, стажистів тощо), отримання інформації від третіх осіб, отримання членами групи аудиту необхідних консультацій, роз’яснень та іншої, у тому числі технічної, допомоги.

5.4.3. Готує робочі документи відповідно до цілей аудиту і проводить інструктаж членів групи аудиту.

5.4.4. Несе відповідальність за проведення всіх етапів аудиту, має навички й досвід керівництва та повноваження для прийняття остаточного рішення відносно аудиту й зроблених у його ході спостережень; у разі необхідності повідомляє головного уповноваженого про фактори, що негативно впливають на незалежність та об’єктивність членів групи аудиту.

5.4.5. Узагальнює висновки й результати спостережень, підготовлені члена-ми групи аудиту в ході його проведення.

5.4.6. Інформує головного уповноваженого про стан виконання графіку проведення внутрішніх аудитів, наявність обмежень у його виконанні.

5.4.7. Доводить до відома керівника аудитованого підрозділу висновки про невідповідності, зауваження, виявлені в ході аудиту.

5.4.8. Погоджує план запобіжних та коригувальних заходів, розроблених аудитованим підрозділом за результатами аудиту.

5.5. Керівник аудитованого підрозділу:

5.5.1. Призначає відповідальних осіб за зв’язок з групою аудиту, сприяє вирішенню завдань з аудиту.

5.5.2. На запит аудиторів надає доступ до необхідної документації.

5.5.3. Бере участь у нарадах, що проводяться групою аудиту.

5.5.4. Затверджує на підставі звіту з аудиту коригувальні дії для усунення невідповідностей та зауважень і направляє їх до відділу дозвільно-погоджу-вальних процедур виконкому міської ради.

5.6. Аудитор:

5.6.1. Несе відповідальність за ефективне й результативне виконання обов’язків, провадить діяльність неупереджено, об’єктивно, без формування власного висновку під впливом третіх осіб та уникає конфлікту інтересів, дотримується норм етики.

5.6.2. Збирає та аналізує докази, у тому числі шляхом спостережень, бесід, необхідні й достатні для формування висновків щодо СУЯ та СУІБ.

5.6.3. Несе відповідальність за забезпечення конфіденційності документів.

5.6.4. Має право на вільний доступ до інформації, що стосується предмету аудиту.

***6. Проведення аудиту та збір об’єктивних доказів***

6.1. Проведення внутрішнього аудиту передбачає збір аудиторських доказів групою аудиту із застосуванням методів, методичних прийомів і процедур, що забезпечують обґрунтованість висновків за його результатами.

6.2. Внутрішні аудитори самостійно визначають методи, методичні при-йоми та процедури, які застосовуються під час внутрішнього аудиту, залежно від його об’єкта та відповідно до вимог процедури й включають:

6.2.1 інтерв'ю, бесіди з працівниками;

6.2.2 аналіз документації;

6.2.3 спостереження за діяльністю;

6.2.4 отримання доказів виконання робочих інструкцій, методик процесів.

6.3. Під аудиторським доказом розуміється зібрана та задокументована надійна й компетентна інформація, яку використовує аудитор з метою обґрун-тування висновків за результатами внутрішнього аудиту.

6.4. Із групою аудиторів можуть бути присутні спостерігачі, які не входять до складу групи з аудиту, вони не можуть протидіяти або чинити вплив на проведення аудиту.

6.5. Якщо в ході аудиту встановлена одна з таких ситуацій:

6.5.1 невідповідність СУЯ та СУІБ вимогам стандартів відповідно ДСТУ ISO 9001:2009 та ISO/ІЕС 27001:2010;

6.5.2 невідповідність послуг, що надаються, установленим законом вимо-гам;

6.5.3 скарги споживачів,

вивчаються причини їх виникнення.

6.6. Після визначення причин виникнення дійсних і потенційних невід-повідностей учасники аудиту приймають рішення про доцільність проведен-ня коригувальних та запобіжних дій.

6.7. Керівник групи аудиту до завершення підготовки звіту має обговорити з членами аудиторської групи:

6.7.1 усі виявлені зауваження та невідповідності, у тому числі ті, які ввій-дуть до висновків;

6.7.2 факти й висновки, за якими потрібне негайне ухвалення рішення;

6.7.3 висновки, що вносяться на обговорення заключної наради.

6.8. У ході внутрішнього аудиту ведуться записи про невідповідності та докази, які їх підтверджують. Заповнюються звіт про проведення внут-рішнього аудиту (додаток 2) та протокол про невідповідність (додаток 3).

6.9. Заключна нарада проводиться під головуванням керівника групи аудиту за участю керівника та відповідальних осіб за функціонування СУЯ та СУІБ аудитованого підрозділу.

6.10. У ході заключної наради:

6.10.1. Керівник групи аудиту інформує про ситуації, виявлені під час проведення аудиту, що вплинули на його результати. Повідомляється про зібраний доказ у ході аудиту, у тому числі шляхом вибірки інформації, а також, про вжиття запобіжних заходів та коригувальних дій (за необхідності).

6.10.2. Обговорюються та, за можливості, урегульовуються будь-які розбіжності у висновках групи аудиту та об’єкта аудиту.

***7. Підготовка звіту***

7.1. Підготовка звіту про підсумки проведення внутрішнього аудиту про-водиться протягом 10 днів після його завершення. Звіт має містити повний, точний, стислий і чіткий опис аудиту. У ньому зазначаються:

7.1.1. Об’єкт аудиту.

7.1.2. Дата, термін та місце проведення.

7.1.3. Склад групи аудиту.

7.1.4. Прізвища представників підрозділу, які брали участь у роботі групи аудиту.

7.1.5. Підстави для проведення аудиту.

7.1.6. Цілі й сфера аудиту.

7.1.7. Критерії аудиту.

7.1.8. Методи аудиту.

7.1.9. Результати аудиту (стислий виклад висновків аудиту).

7.1.10. Вимоги до конфіденційності.

7.1.11. Невідповідності, зауваження та рекомендації.

7.1.12. Неврегульовані розбіжності у висновках групи та об’єкта аудиту (за наявності);

7.1.13. Висновки за результатами аудиту.

7.2. Звіт затверджується керівником групи аудиту й передається головному уповноваженому для аналізу та прийняття рішень за результатами аудиту.

7.3. Після затвердження копії звіту направляються в аудитовані підрозділи та заступникам міського голови, керуючій справами виконкому міської ради відповідно до розподілу обов’язків.

7.4. Документи з аудитів зберігаються в окремій справі у відділі дозвільно-погоджувальних процедур виконкому міської ради , відповідно до термінів, що регламентуються Номенклатурою справ відділу.

***8. Контроль виконання заходів, розроблених***

***за наслідками результатів аудиту***

8.1. Керівник аудитованого підрозділу протягом 3 днів після отримання звіту має надати план коригувальних дій щодо усунення виявлених невідповідностей (у разі їх наявності) до відділу дозвільно-погоджувальних процедур виконкому міської ради.

8.2. Керівник групи аудиту або призначений для цієї мети аудитор має одержати коригувальні дії, розглянути їх достатність і повноту, переконатися в тому, що вони виконуються відповідно до запропонованого плану, визначити, що ухвалені заходи виявилися своєчасними й ефективними.

8.3. Підтвердженням завершення виконання коригувальних дій може бути направлення письмової інформації або проведення повторного (контрольного) аудиту.

8.4. При проведенні аудитів з невеликим обсягом інформації допускається розміщення виявлених невідповідностей, коригувальних дій і відмітки про їх виконання в одному документі – листі реєстрації зауважень.

8.5. Результатами аудиту є усунення невідповідностей чи здійснення коригувальних дій. У разі виявлення невідповідностей, на кожну з них аудитор заповнює лист реєстрації невідповідностей у двох примірниках: один з них надається до відділу дозвільно-погоджувальних процедур виконкому міської ради, другий – залишається в аудитованому підрозділі.

8.6. Аудитори перевіряють виконання коригувальних дій у зазначений термін і роблять запис у листі реєстрації невідповідностей у примірнику відділу дозвільно-погоджувальних процедур виконкому міської ради.

8.6. Дані про внутрішні аудити включаються до звіту про функціонування СУЯ та СУІБ за звітний період.

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