Додаток 3
до розпорядження голови
районної в місті ради
від 09.11.2017 № 242-р

Методика
управління ризиками у виконкомі Довгинцівської районної в місті ради

1. Загальні положення

1.1. Методика управління ризиками у виконкомі Довгинцівської районної в місті ради (надалі – Методика) визначає основні засади побудови системи управління ризиками, загальні аспекти впровадження єдиної методологічної бази по оцінці ризиків, принципи взаємодії структурних підрозділів виконавчого комітету районної в місті ради в процесі управління ризиками.

1.2. Метою методики є створення ефективної системи управління ризиками для виконання поточних та стратегічних цілей виконкому районної в місті ради із застосуванням відповідних політик, методів і засобів управління та контролю за ризиками, що генеруються зовнішнім середовищем, структурою активів і процесами виконкому районної в місті ради.

1.3. Основними завданнями Методики є:

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

1.4. Управління інформаційними ризиками включає:

- виявлення ризиків;
- проведення оцінки ризиків з точки зору їх впливу на діяльність виконкому районної в місті ради та ймовірності їх виникнення;
- визначення характерних ознак ризиків;
- здійснення моніторингу (контролю) ризиків, проведення аналізу їх впливу на виконання основних процесів, наслідків їх виникнення, ймовірності виникнення певного ризику в подальшому;
- вибір форми управління ризиками;
- інформування керівництва та персоналу про ризики та дії щодо управління ними.

1.5. Методика розповсюджується на всі структурні підрозділи виконавчого комітету районної в місті ради, вимоги її є обов’язковими для працівників виконкому районної в місті ради.

2. Терміни та визначення

Ризик – можлива подія, дія або умова, котрі, у разі виникнення, можуть мати негативний вплив на діяльність виконкому районної в місті ради.

Управління ризиками – розроблення та здійснення оптимальних заходів для запобігання виникненню ризиків та ліквідації наслідків їх виникнення.

Оцінка ризику – процес виявлення ризику та визначення можливих наслідків його виникнення.

Аналіз ризику – систематичний процес визначення величини ризику.

Загроза – потенційна причина інциденту, що може заподіяти шкоду системі або виконкому.

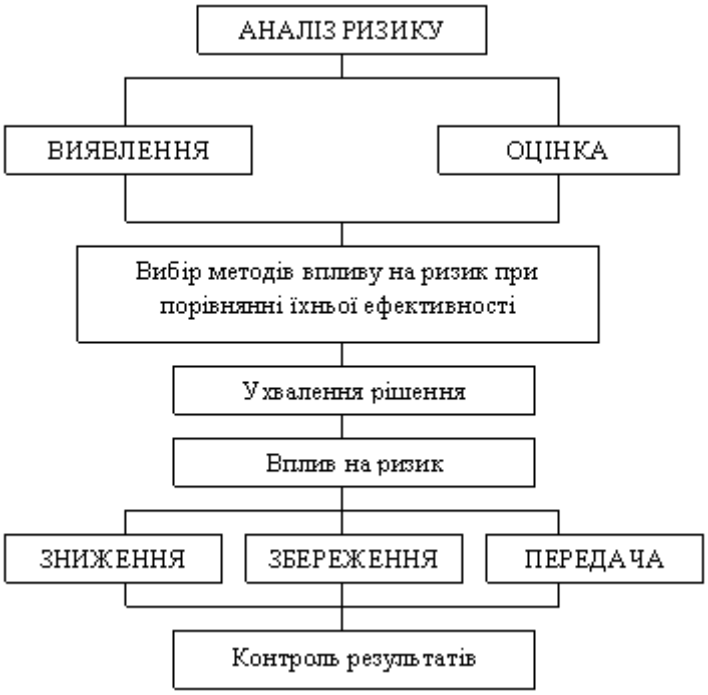
Уразливість – слабкість одного чи декількох активів, що може бути використана однією чи декількома загрозами.

Актив (ресурс) – усе, що має цінність для виконкому, ресурси виконкому (матеріальні й нематеріальні).

3. Аналіз ризиків

3.1. Ризиком інформаційної безпеки вважається ймовірність того, що визначена загроза, впливаючи на вразливості ресурсу або групи ресурсів, може спричинити шкоду виконкому районної в місті ради.

3.2. Структура процесу поводження з ризиками інформаційної безпеки схематично зображена на малюнку 1.



Мал. 1. Процес управління ризиками

4. Ідентифікація загроз та уразливостей

4.1. Загрози потенційно можуть завдати шкоди ресурсам системи управління інформаційною безпекою, зокрема інформації, персоналу, громадянам, обладнанню, процесам і програмно-технічним комплексам. Загрози можуть мати природні та людські джерела та бути випадковими або навмисними. Ідентифікації потребують як випадкові, так і навмисні джерела загроз. Загрози можуть бути ідентифіковані в загальному вигляді або за типами (наприклад, неавторизовані дії, фізичні чи технічні пошкодження тощо).

4.2. До ідентифікації загроз залучаються власники процесів та користувачі.

4.3 Типовий перелік загроз:

- природні – землетрус, повінь, ураган, попадання блискавки, вплив пилу, статичної електроенергії тощо;

- випадкові – пожежа, затоплення, несправності в системі енергозабезпечення (водозабезпечення), апаратні відмови, коливання напруги, помилки обслуговуючого персоналу, використання програмного забезпечення несанкціонованими користувачами, технічні несправності мережевих компонентів, помилки операторів, пошкодження ліній, відправка повідомлень на помилкову адресу тощо;

- навмисні дії – навмисне пошкодження системи кондиціонування повітря, крадіжка, несанкціоноване використання носіїв даних, помилки при обслуговуванні, програмні перебої, несанкціоноване проникнення, використання програмного забезпечення несанкціонованим способом, незаконне використання програмного забезпечення, несанкціонований доступ до мережі, пошкодження ліній, перехват інформації, несанкціоноване проникнення до засобів зв’язку, помилки користувачів, неналежне використання ресурсів тощо.

4.4. Після ідентифікації джерела (хто? чи що? є причиною загрози) та об’єкта (на який з елементів активу може діяти загроза) необхідно оцінити ймовірність її реалізації.

При цьому слід враховувати:

- частоту появи загрози (як часто вона може виникати згідно зі статистичними, дослідними та іншими даними, якщо такі є);

- мотивацію, можливості та ресурси, необхідні потенційному порушнику та, можливо, є в його розпорядженні;

- ступінь привабливості та вразливості інформаційних активів з точки зору потенційного порушника та джерела навмисної загрози;

- географічні фактори (наявність поблизу хімічних чи нафтопереробних підприємств, можливість виникнення екстремальних погодних умов, фактори, що можуть призвести до помилок персоналу, вихід з ладу обладнання тощо).

Після завершення оцінки загроз складається перелік ідентифікованих загроз, активів чи груп активів, схильних до цих загроз.

Ідентифікація уразливостей відбувається під час їх оцінки, у яких можуть бути реалізовані можливі загрози. До ідентифікації уразливостей залучаються власники чи користувачі активів, спеціалісти з обслуговування пристроїв, експерти з програмних та апаратних засобів систем інформаційних технологій.

Перелік типових уразливостей:

- незахищені підключення (наприклад Інтернет);
- некваліфіковані користувачі;
- неправильний вибір та використання пароля доступу;
- відсутність належного контролю доступу;
- відсутність резервних копій інформаційних даних чи програмного забезпечення тощо.

4.7. Ступінь уразливості слід оцінювати у відношенні кожної загрози, що може використовувати цю уразливість у конкретній ситуації (наприклад,

система може бути уразливою до загрози несанкціонованого проникнення при ідентифікації користувача та несанкціонованого використання ресурсів).

Вразливості, які можуть бути використані загрозами для впливу на ресурси системи управління інформаційною безпекою та процеси, також повинні бути ретельно розглянуті та ідентифіковані.

4.8. Після завершення ідентифікації уразливостей складається їх перелік та проводиться оцінка ступеня вірогідності можливої реалізації зазначених уразливостей (висока, середня, низька). Перелік ризиків оформлюється у наступному рекомендованому вигляді:

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
1	*2*	*3*	*4*	*5*
Імідж та репутація				
Персонал				
Інформація				
Приміщення				
Обладнання				
……				

Остаточна форма документування записів за ідентифікацією та оцінкою ризиків визначається та затверджується головним уповноваженим з питань інформаційної безпеки виконкому.

5 Оцінка ризиків

5.1. Оцінка ризиків проводиться з метою ідентифікації та вибору обґрунтованих методів захисту безпеки. Величина ризику визначається цінністю активів, схильних до ризику, вірогідністю реалізації загроз, здатних негативно впливати на ділову активність; можливістю використання уразливостей ідентифікованими загрозами, наявністю діючих або запланованих заходів захисту, використання яких може знизити рівень ризику.

5.2. Методологія оцінки ризиків може бути кількісною, якісною, або їх комбінацією. Якісна оцінка часто використовується спочатку для визначення загального рівня ризику й визначення основних ризиків. Кількісна оцінка ризиків є більш складною та потребує більше часу й ресурсів. Однак така оцінка буде дуже корисною у випадках, коли рішення щодо оброблення ризиків буде залежати від вартості заходів безпеки, які можуть бути більшими, ніж фінансові втрати інциденту інформаційної безпеки.

5.3. Визначення конкретних величин для параметрів оцінки повинно виконуватися з урахуванням досвіду працівників виконкому районної в місті ради, вимог нормативно-правових актів, історії попередніх інцидентів інформаційної безпеки, відомих випадків порушення інформаційної безпеки, досвіду інших установ тощо. Оцінка ризиків документується у вигляді звіту для кожного процесу:

Звіт оцінки ризиків для процесу

_____

(назва)

Загроза/ вразливість	***Оцінка ймовірності реалізації загрози з використанням вказаної вразливості***	***Оцінка впливу реалізації загрози на цілісність***	***Оцінка впливу реалізації загрози на конфіденційність***	***Оцінка впливу реалізації загрози на доступність***	***Оцінка впливу реалізації загрози на спостережність***	***Рівень ризику за окремою парою загроза/ вразливість***
Загальний ризик процесу						

Рекомендується використовувати такі шкали для оцінки ризиків:

5.4.1. Для оцінки ймовірності реалізації загроз:

Оцінка ймовірності	***Опис***
1	Виникнення інциденту практично неможливо
2	Виникнення інциденту малоймовірне (не частіше ніж 1 раз на рік)
3	Виникнення інциденту ймовірне до 1 разу на 3 місяці

4	Виникнення інциденту ймовірне до 1 разу на тиждень
5	Виникнення інциденту ймовірне до 1 разу на добу

5.4.2. Для величини наслідків реалізації загрози, вплив на цілісність:

Оцінка рівня наслідків	***Опис***
1	Практично не призводить до наслідків з фінансовими втратами
2	Призводить до незначних фінансових втрат (визначити суму) та має незначний вплив на репутацію виконкому
3	Призводить до значних фінансових втрат (визначити суму) та має значний вплив на репутацію виконкому
4	Призводить до великих фінансових втрат (визначити суму), має значний вплив на репутацію виконкому і може призвести до зупинки виконання процесу
5	Призводить до зупинки виконання процесу і порушує законодавство України

5.4.3. Для величини наслідків реалізації загрози, вплив на конфіденційність:

Оцінка рівня наслідків	***Опис***
1	Практично не призводить до розкриття конфіденційної інформації
2	Призводить до розкриття окремих документів, які відносяться до конфіденційних, документів для службового користування, персональних даних і не призводить до фінансових втрат
3	Призводить до розкриття окремих документів, які відносяться до конфіденційних, документів для службового користування, персональних даних і призводить до незначних фінансових втрат
4	Призводить до розкриття документів, які відносяться до таємних, персональних даних і призводить до значних фінансових втрат, має значний вплив на репутацію виконкому і може призвести до зупинки виконання процесу
5	Призводить до зупинки виконання процесу і порушує законодавство України

5.4.4. Для величини наслідків реалізації загрози, вплив на доступність:

Оцінка	***Опис***

рівня наслідків	
1	Практично не впливає на доступність
2	Вплив на доступність незначний (не більше1/10 від максимально допустимого часу простою для цього процесу)
3	Вплив на доступність середній (не більше – від максимально допустимого часу простою для цього процесу)
4	Вплив на доступність значний (до максимально допустимого часу простою для цього процесу)
5	Призводить до зупинки процесу на тривалий час, який перевищує максимально допустимий час простою

5.4.5. Для величини наслідків реалізації загрози, вплив на спостережність:

Оцінка рівня наслідків	***Опис***
1	Практично не впливає
2	Вплив незначний
3	Призводить до неможливості відстежити частину дій виконавців процесу
4	Призводить до неможливості відстежити дії виконавців і адміністраторів процесу чи програмно-технічного комплексу
5	Призводить до неможливості відстежити дії виконавців і адміністраторів процесу чи програмно-технічного комплексу, може призвести до зупинки процесу, має вплив на репутацію виконкому і порушує законодавство України

5.5. Результатом оцінки ризиків є перелік ризиків для кожного можливого випадку розкриття, зміни, обмеження доступності та руйнування інформації в діючій системі інформаційних технологій. Цей перелік використовується при ідентифікації ризику, на який слід звертати увагу в першу чергу при виборі захисних заходів. Рекомендується документувати узагальнений звіт про оцінку ризиків відповідно до форми:

№ з/п	***Розпорядник активу***	***Актив або група активів***	***Ризик***	***Рівень ризику***
1	***2***	***3***	***4***	***5***

Узагальнений звіт про оцінку ризиків погоджується головним уповноваженим з питань інформаційної безпеки виконкому та доводиться до відома всіх структурних підрозділів, по яким проводилась оцінка ризиків.

6. Вибір заходів захисту

6.1. Основою для ідентифікації заходів захисту, необхідних для забезпечення інформаційної безпеки, є результати оцінки рівня ризиків.

6.2. Область використання заходів захисту включає:

- фізичне навколишнє середовище;
- обслуговуючий персонал, адміністрація;
- апаратні засоби (програмне забезпечення);
- засоби забезпечення зв'язку (комунікації).

6.3. Для ідентифікації заходів захисту необхідно розглянути уразливості системи (активів), що потребують захисту, та види загроз, які можуть реалізуватися при наявності цих уразливостей; економічну складову (вартість) того чи іншого заходу.

6.4. До типових видів зниження рівня ризиків належать:

- уникнення ризику;
- зниження рівня загроз;
- зниження ступеня вразливості системи інформаційних технологій;
- зниження можливого впливу небажаних подій;
- моніторинг виникнення небажаних подій, реагування на їх появу та усунення їх наслідків.

6.5. Вибір заходів захисту повинен включати в себе комбінацію організаційних та технічних заходів. Як організаційні розглядаються заходи, що забезпечують фізичну (потужність внутрішніх стін будівель, використання кодових замків, систем пожежогасіння, охоронних служб), персональну (перевірка осіб при прийомі на роботу, контроль за роботою персоналу, реалізація програм знання та розуміння заходів захисту) та адміністративну (безпечні способи ведення документації, наявність методів розробки та впровадження прикладних програм, процедур обробки інцидентів у випадках порушення системи безпеки.

Технічні заходи безпеки передбачають захист апаратних засобів, програмного забезпечення та системи зв'язку (комунікації). При цьому вибір заходів здійснюють у відповідності до ступеня ризику для забезпечення функціональної придатності та надійності системи безпеки.

Приклад оцінки ризику

Ризик: неможливість здійснювати діяльність унаслідок відсутності Інтернет-з'єднання

Опис ризику

Підключення до мережі Інтернет застосовується у виконкомі районної в місті ради під час:

- отримання/відправлення електронної пошти;
- здійснення перегляду/пошуку інформації в мережі Інтернет;
- підтримки з'єднання з базами даних державних служб;
- роботи та оновлення програмного забезпечення.

Оцінка ймовірності ризику виникнення інциденту

Таблиця 1

Оцінка ймовірності	***Опис***
1	Виникнення інциденту практично неможливе
2	Виникнення інциденту малоймовірне (не частіше ніж 1 раз на рік)
3	Виникнення інциденту ймовірне до 1 разу на 3 місяці
4	Виникнення інциденту ймовірне до 1 разу на тиждень
5	Виникнення інциденту ймовірне до 1 разу на добу

В усіх структурних підрозділах виконкому районної в місті ради. використовується Інтернет-з'єднання та налагоджені процедури швидкого реагування на його відновлення. Також є можливість здійснювати діяльність без нього або використовувати інші безпечні Інтернет-з'єднання. Але ризик виникнення інциденту все ж існує через наявність «людського фактору». За цим критерієм ризик дорівнює **двом балам** - виникнення інциденту мало-ймовірне (не частіше 1 разу на рік).

Оцінка рівня наслідків з фінансовими втратами або впливу на репутацію:

Таблиця 2

Оцінка рівня наслідків	***Опис***
1	Практично не призводить до наслідків з фінансовими втратами
2	Призводить до незначних фінансових втрат та має незначний вплив на репутацію виконкому
3	Призводить до значних фінансових втрат та має значний вплив на репутацію виконкому
4	Призводить до великих фінансових втрат, має значний вплив на репутацію виконкому і може призвести до зупинки виконання процесу
5	Призводить до зупинки виконання процесу і порушує законодавство України

У разі припинення Інтернет-з'єднання структурні підрозділи виконкому районної в місті ради можуть виконувати роботу або перенести строки її виконання без фінансових втрат чи втрат репутації. За цим критерієм ризик отримує **один бал** - практично не призводить до наслідків з фінансовими втратами.

Оцінка рівня загрози розкриття конфіденційної інформації при виникненні інциденту:

Таблиця 3

Оцінка рівня наслідків	***Опис***
1	Практично не призводить до розкриття конфіденційної інформації
2	Призводить до розкриття окремих документів, які відносяться до конфіденційних, документів для службового користування, персональних даних і не призводить до фінансових втрат
3	Призводить до розкриття окремих документів, які відносяться до конфіденційних, документів для службового користування, персональних даних і призводить до незначних фінансових втрат
4	Призводить до розкриття документів, які відносяться до таємних, персональних даних і призводить до значних фінансових втрат, має значний вплив на репутацію виконкому і може призвести до зупин-ки виконання процесу
5	Призводить до зупинки виконання процесу і порушує законодавство України

Існуючі процедури захисту конфіденційної інформації (обмеження доступу, технічні та програмні засоби тощо) попереджують виникнення інциденту розкриття конфіденційної інформації. Зокрема втрата Інтернет-з'єднання не впливає на можливість розкриття конфіденційної інформації. За цим критерієм ризик отримує **один бал** - практично не призводить до розкриття конфіденційної інформації.

Оцінка рівня впливу на доступність при виникненні інциденту:

Таблиця 4

Оцінка рівня наслідків	***Опис***
1	Практично не впливає на доступність
2	Вплив на доступність незначний (не більше1/10 від максимально допустимого часу простою для цього процесу)
3	Вплив на доступність середній (не більше – від максимально допустимого часу простою для цього процесу)
4	Вплив на доступність значний (до максимально допустимого часу простою для цього процесу)
5	Призводить до зупинки процесу на тривалий час, який перевищує максимально допустимий час простою

Визнаючи, що ризик має місце, також мається на увазі, що може існувати вплив на доступність до інформаційних ресурсів, необхідних для здійснення діяльності. Оскільки існують відповідні домовленості та процедури, гарантується, що в цьому випадку простій для процесу не буде більшим від максимально допустимого, рівень наслідків дорівнює **трьом балам.**

Оцінка рівня впливу на спостережність при виникненні інциденту:

Таблиця 5

Оцінка рівня наслідків	***Опис***
1	Практично не впливає
2	Вплив незначний
3	Призводить до неможливості відстежити частину дій виконавців процесу
4	Призводить до неможливості відстежити дії виконавців і адміністраторів процесу чи програмно-технічного комплексу
5	Призводить до неможливості відстежити дії виконавців і адміністраторів процесу чи програмно-технічного комплексу, може призвести до зупинки процесу, має вплив на репутацію виконкому і порушує законодавство України

Відсутність Інтернет-з’єднання не впливає на можливість відстеження дій виконавців процесу, оскільки воно може вестися та ведеться без застосування Інтернет-з’єднання. За цим критерієм ризик отримує один бал-практично не впливає на спостережність при виникненні інциденту.

Підсумок: таким чином сума всіх балів складає **8 балів**, що дорівнює **середньому** рівню ризику.

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