*ЗАТВЕРДЖЕНО*

*Розпорядження міського голови*

*02.03.2015 №75-р*

***МЕТОДИКА УПРАВЛІННЯ РИЗИКАМИ***

***1. Загальні положення***

1.1. Методика управління ризиками (надалі – Методика) визначає основні засади побудови системи управління ризиками, загальні аспекти впровадження єдиної методологічної бази з їх оцінки, принципи взаємодії відділів, управлінь, інших виконавчих органів міської ради в процесі управління ризиками.

1.2. Метою Методики є створення ефективної системи управління ризи-ками для виконання поточних і реалізації стратегічних цілей виконкому міської ради із застосуванням відповідних політик, методів і засобів управління та кон-тролю за ризиками, що генеруються зовнішнім середовищем, структурою акти-вів і процесами виконкому міської ради.

1.3. Основними завданнями Методики є:

1.3.1 установлення ефективної системи підтримки ухвалення управлін-ських рішень з урахуванням рівня ризиків у сфері інформаційної безпеки;

1.3.2 забезпечення здійснення діяльності виконкому міської ради у відповідності до встановлених політик, процедур і регламентів;

1.3.3 зниження рівня очікуваних і неочікуваних ризиків.

1.4. Управління інформаційними ризиками включає:

1.4.1 їх виявлення;

1.4.2 вивчення оцінки їх впливу на діяльність виконкому міської ради та ймовірності їх виникнення;

1.4.3 визначення характерних ознак ризиків;

1.4.4 здійснення моніторингу (контролю) ризиків, проведення аналізу їх впливу на виконання основних процесів, наслідків їх виникнення, ймовірності виникнення певного ризику в подальшому;

1.4.5 вибір форми управління ризиками;

1.4.6 інформування керівництва та персоналу про ризики й дії щодо управління ними.

1.5. Методика розповсюджується на всі відділи, управління, інші вико-навчі органи міської ради, її вимоги є обов’язковими для працівників виконко-му міської ради.

***2. Терміни та визначення***

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

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

**Оцінка ризику** – процес виявлення ризику та визначення можливих нас-лідків його виникнення.

**Аналіз ризику** – систематичний процес визначення величини ризику.

**Загроза** – потенційна причина інциденту, що може заподіяти шкоду сис-темі або організації.

**Уразливість** – слабкість одного чи декількох активів, що може бути ви-

користана однією чи декількома загрозами.

***3. Аналіз ризиків***

3.1. Ризиком інформаційної безпеки вважається ймовірність того, що ви-значена загроза, впливаючи на вразливості ресурсу або групи ресурсів, може спричинити шкоду виконкому міської ради.

3.2.

Аналіз ризику

Виявлення

Оцінка

Вибір методів впливу на ризик при порівнянні їх ефективності

Ухвалення рішення

Вплив на ризик

Зниження

Збереження

Передача

Контроль результатів

***4. Ідентифікація загроз та уразливостей***

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

4.2. До ідентифікації загроз залучаються власники активів та користувачі.

4.3. Типовий перелік загроз:

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

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

4.3.3 навмисні дії – навмисне пошкодження системи кондиціонування по-

вітря, крадіжка, несанкціоноване використання носіїв даних, помилки при обслуговуванні, програмні перебої, несанкціоноване проникнення, викорис-тання програмного забезпечення несанкціонованим способом, незаконне ви-користання 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’єк-та (на який з елементів активу може діяти загроза) загрози необхідно оцінити ймовірність її реалізації. При цьому слід ураховувати:

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

4.4.2 мотивацію, можливості та ресурси, необхідні потенційному поруш-нику та, можливо, є в його розпорядженні;

4.4.3 ступінь привабливості та вразливості інформаційних активів з погляду потенційного порушника та джерела навмисної загрози;

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

Після завершення оцінки загроз складається реєстр ідентифікованих заг-роз, активів чи груп активів, схильних до цих загроз.

4.5. Ідентифікація уразливостей відбувається під час оцінки уразливостей, 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.

4.6. Перелік типових уразливостей:

4.6.1 незахищені підключення (наприклад Інтернет);

4.6.2 некваліфіковані користувачі;

4.6.3 витік, розголошення або втрата інформації;

4.6.4 неправильний вибір та використання пароля доступу;

4.6.5 відсутність належного контролю доступу;

4.6.6 відсутність резервних копій інформаційних даних чи програмного забезпечення тощо.

4.7. Ступінь уразливості слід оцінювати відносно кожної загрози, що може використовувати цю уразливість у конкретній ситуації (наприклад, сис-тема може бути уразливою до загрози несанкціонованого проникнення при ідентифікації користувача та несанкціонованого використання ресурсів).

4.8. Після завершення ідентифікації уразливостей складається їх реєстр та проводиться оцінка ступеня вірогідності можливої реалізації зазначених уразливостей (висока, середня, низька).

***5. Оцінка ризиків***

5.1. Оцінка ризиків проводиться з метою ідентифікації та вибору обґрун-

тованих методів захисту безпеки. Величина ризику визначається цінністю акти-вів, 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 використовується для визначення загального рівня ризику й основних ризиків. Кількісна оцінка - у випадках, коли оброблення ризиків залежить від вартості заходів безпеки, які можуть бути більшими, ніж фінансові втрати інциденту інформаційної безпеки.

5.3. Визначення конкретних величин для параметрів оцінки має вико-нуватися з урахуванням досвіду працівників виконкому міської ради, вимог нормативно-правових актів, історії попередніх інцидентів інформаційної безпе-ки, відомих випадків порушення інформаційної безпеки, досвіду інших установ тощо. Оцінка ризиків документується у вигляді таблиці для кожного процесу. Приклад оцінки ризику наведено в додатку.

5.4. Рекомендовані шкали для оцінки ризиків:

5.4.1. Для оцінки ймовірності реалізації загроз:

|  |  |  |
| --- | --- | --- |
| ***Оцінка ймовірності*** | ***Опис*** | |
| 1 | Виникнення інциденту | практично неможливе |
| 2 | малоймовірне (не частіше 1 разу на рік) |
| 3 | ймовірне до 1 разу на 3 місяці |
| 4 | ймовірне до 1 разу на тиждень |
| 5 | 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 втрата-ми |
| 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 й може призвести до зупинки виконання процесу |
| 5 | Призводить до зупинки виконання процесу й порушує норми  законодавства України |

5.4.3. Для величини наслідків реалізації загрози: вплив на кон-фіденційність:

|  |  |
| --- | --- |
| ***Оцінка рівня наслідків*** | ***Опис*** |
| 1 | Практично не призводить до розкриття конфіденційної ін-формації |
| 2 | Призводить до розкриття окремих документів, що належать до конфіденційних, для службового користування, персональних даних, і не призводить до фінансових втрат |
| 3 | Призводить до розкриття окремих документів, що належать до конфіденційних, для службового користування, персональних даних, і призводить до незначних фінансових втрат (визначити суму) |
| 4 | Призводить до розкриття документів, що належать до конфі-денційних, персональних даних, і до значних фінансових втрат (визначити суму), має значний вплив на репутацію виконкому міської ради та може призвести до зупинки виконання процесів діяльності |
| 5 | Призводить до зупинки виконання процесів і порушує чинне законодавство України |

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

|  |  |
| --- | --- |
| ***Оцінка рівня наслідків*** | ***Опис*** |
| 1 | Практично не впливає на доступність |
| 2 | Вплив на доступність незначний (не більше 1/10 від мак-симально допустимого часу простою для цього процесу) |
| 3 | Вплив на доступність середній (не більше від максимально до-пустимого часу простою для цього процесу) |
| 4 | Вплив на доступність значний (близький до максимально допустимого часу простою для цього процесу) |
| 5 | Призводить до зупинки процесу на тривалий час, що переви-щує максимально допустимий час простою |

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

|  |  |
| --- | --- |
| ***Оцінка рівня наслідків*** | ***Опис*** |
| ***1*** | ***2*** |
| 1 | Практично не впливає |
| 2 | Вплив незначний |
| 3 | Призводить до неможливості відстежити частину дій ви-конавців процесу |
| 4 | Призводить до неможливості відстежити дії виконавців і адміністраторів процесу чи програмно-технічного комплексу |

|  |  |
| --- | --- |
| ***1*** | ***2*** |
| 5 | Призводить до неможливості відстежити дії виконавців і адміністраторів процесу чи програмно-технічного комплексу, може призвести до зупинки процесу, має вплив на репутацію виконкому та порушує чинне законодавство України |

5.5. Результатом оцінки ризиків є реєстр 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 за-хисних заходів.

***6. Вибір заходів захисту***

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

6.2. Область використання заходів захисту включає:

6.2.1 фізичне навколишнє середовище;

6.2.2 обслуговуючий персонал, адміністрацію;

6.2.3 апаратні засоби (програмне забезпечення);

6.2.4 засоби забезпечення зв’язку (комунікації).

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

6.4. До типових видів зниження рівня ризиків належать:

6.4.1 уникнення ризику;

6.4.2 зниження рівня загроз;

6.4.3 зниження ступеня вразливості системи інформаційних технологій;

6.4.4 зниження можливого впливу небажаних подій;

6.4.5 моніторинг виникнення небажаних подій, реагування на їх появу та усунення їх наслідків.

6.5. Вибір заходів захисту має включати комбінацію організаційних (не- технічних) 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 впрова-дження прикладних програм, процедур обробки інцидентів у випадках пору-шення системи безпеки) безпеку.

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

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