ГОЛОВА ДОВГИНЦІВСЬКОЇ РАЙОННОЇ В МІСТІ РАДИ

Р О З П О Р Я Д Ж Е Н Н Я

24.11.2021 м. Кривий Ріг № 345-р

Про затвердження нормативної документації системи управління інформаційною безпекою

З метою впорядкування нормативної документації системи управління інформаційною безпекою виконкому Довгинцівської районної в місті ради, відповідно до вимог стандарту ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги», забезпечення її функціонування та підвищення ефективності роботи виконкому районної в місті ради, керуючись Законом України «Про місцеве самоврядування в Україні», рішенням Криворізької міської ради від 31.03.2016 № 381 «Про обсяг і межі повноважень районних у місті рад та їх виконавчих органів» зі змінами:

1. Затвердити нормативну документацію системи управління інформаційною безпекою, а саме:

1.1. Настанову з інформаційної безпеки виконкому Довгинцівської районної в місті ради (додаток 1);

1.2. Політики і принципи інформаційної безпеки виконкому Довгинцівської районної в місті ради (додаток 2);

1.3. План зниження ризиків системи управління інформаційною безпекою у виконкомі Довгинцівської районної в місті ради (додаток 3);

1.4. Методику виявлення та реєстрації інцидентів інформаційної безпеки у виконкомі Довгинцівської районної в місті ради (додаток 4);

1.5. Положення про застосування цілей заходів інформаційної безпеки у виконкомі Довгинцівської районної в місті ради (додаток 5);

1.6. Політику у сфері інформаційної безпеки виконкому Довгинцівської районної в місті ради (додаток 6);

1.7. Процедуру управління інформаційними активами виконкому Довгинцівської районної в місті ради (додаток 7);

1.8. Реєстр інформаційних активів виконкому Довгинцівської районної в місті ради (додаток 8);

1.9. Реєстр ризиків виконкому Довгинцівської районної в місті ради (додаток 9);

1.10. Методику управління ризиками у виконкомі Довгинцівської районної в місті ради (додаток 10);

1.11. Положення про придбання, розробку та обслуговування інформаційних систем (додаток 11);

1.12. Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради (додаток 12).

2. Вважати такими, що втратили чинність розпорядження голови Довгинцівської районної в місті ради:

- від 14.11.2017 № 251-р «Про затвердження Настанови з інформаційної безпеки виконкому Довгинцівської районної в місті ради»;

- від 09.11.2017 № 239-р «Про затвердження Політик і принципів інформаційної безпеки виконкому Довгинцівської районної в місті ради»;

- від 09.11.2017 № 238-р «Про затвердження Плану зниження ризиків системи управління інформаційною безпекою у виконкомі Довгинцівської районної в місті ради»;

- від 09.11.2017 № 244-р «Про затвердження Методики виявлення та реєстрації інцидентів інформаційної безпеки у виконкомі Довгинцівської районної в місті ради»;

- від 15.11.2017 № 253-р «Про затвердження Положення про застосування цілей заходів інформаційної безпеки у виконкомі Довгинцівської районної в місті ради»;

- від 09.11.2017 № 241-р «Про Політику у сфері інформаційної безпеки та Процедуру управління інформаційними активами виконкому Довгинцівської районної в місті ради»;

- від 09.11.2017 № 242-р «Про затвердження внутрішньої документації системи управління інформаційною безпекою»;

- від 09.11.2017 № 240-р «Про затвердження Положення про придбання, розробку та обслуговування інформаційних систем»;

- від 09.11.2017 № 243-р «Про затвердження Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради».

3. Координацію роботи щодо виконання розпорядження покласти на відділ інформаційних технологій (Луценко Ю.І.), контроль – на керуючого справами виконкому Гижка О.О.

Голова районної в місті ради ***Ігор Ратінов***

Додаток 1
до розпорядження голови
районної в місті ради
від 24.11.2021 № 345-р

Настанова
з інформаційної безпеки виконкому
Довгинцівської районної в місті ради

Зміст

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: (056) 4701100.

Факс: (056) 4701099.

Адреса електронної пошти (email): 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 17 січня 2018 року № 55 «Деякі питання документування управлінської діяльності»;
- Рішення Криворізької міської ради від 31.03.2016 № 381 «Про обсяг і межі повноважень районних у місті рад та їх виконавчих органів» зі змінами;
- рішення виконкому Криворізької міської ради від 12.09.2018 № 428 «Про затвердження Інструкції з діловодства в органах місцевого самоврядування міста» зі змінами;
- рішення Довгинцівської районної в місті ради від 24.02.2021 № 28 «Про затвердження Регламенту Довгинцівської районної в місті ради VIII скликання»;
- рішення виконкому Довгинцівської 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;
- від 17.04.2019 № 143 «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

Політику у сфері інформаційної безпеки виконкому Довгинцівської районної в місті ради (додаток 6) 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 вебсайт виконкому Довгинцівської районної в місті ради, 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 24.02.2021 № 28 «Про затвердження Регламенту Довгинцівської районної в місті ради VIII скликання».

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 відповідно 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 12.09.2018 № 428 «Про затвердження Інструкції з діловодства в органах місцевого самоврядування міста» зі змінами 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, посадова 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 ***Олександр 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
А11. 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

А12. 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

А13. Управління інцидентами

Процедура виявлення та реєстрації інцидентів
Журнал реєстрації інцидентів ІБ
Журнал реєстрації скарг і пропозицій ІБ

А14. Управління безперервністю робочих процесів

Процедура управління безперервністю робочих процесів
Плани відновлення робочих процесів
Записи про тестування планів відновлення

А15. 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

Додаток 2
до розпорядження голови
районної в місті ради
від 24.11.2021 № 345-р

Політики і принципи
інформаційної безпеки виконкому Довгинцівської районної в місті ради

Зміст

13. Принципи поводження з ключами від приміщень, а також канцелярських шаф.

14. Реєстрація змін у документації.

15. Принципи класифікації інформації.

I. Вступ

Інформаційну безпеку регулюють Закони України: «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», «Про захист суспільної моралі», «Про доступ до публічної інформації».

Для забезпечення юридичних вимог використовуються стандарти ДСТУ ISO/IEC 27001:2015 та ДСТУ ISO/IEC 9001:2015.

II. Мета

Метою розробки даного документу є усвідомлення працівниками виконавчого комітету районної в місті ради і суб'єктів, які діють на користь виконкому, проблем інформаційної безпеки та щоденного використання його при виконанні робіт у виконавчому комітеті районної в місті ради або на користь виконкому зовнішніми суб'єктами.

III. Сфера застосування

Застосування Політики у сфері інформаційної безпеки у роботі виконкому Довгинцівської районної в місті ради, а також принципів інформаційної безпеки є обов'язковими до виконання в усіх структурних підрозділах виконкому.

IV. Терміни

1. Типи інформації.

Усна інформація – переказана, під час розмови.

Відтворена аудіо-, відеотехнікою.

Переслана поштою.

Передана електронним шляхом.

Збережена в електронній формі.

Зображена на екрані монітора.

Надрукована, або записана на папері.

2. Терміни і визначення.

Активи – все те, що має вартість для організації.

Безпека інформації - збереження секретності, інтегральності і доступності інформації.

Секретність – властивість, яка полягає в тому, що інформація не є доступною або виявленою не уповноваженим особам, суб'єктам, або процесам.

Інтегральність – властивість, яка полягає у запевненні точності і повноти активів.

Доступність – властивість бути доступним і корисним на вимогу уповноваженого суб'єкта.

Система управління інформаційною безпекою (СУІБ) – це частина цілісної системи управління, яка ґрунтується на підході, що виникає з ризику, стосовно розробки, впровадження, експлуатації, моніторингу, підтримки і вдосконалення безпеки інформації.

Політика СУІБ - вираження керівництвом загальних намірів і напрямків діяльності.

Засоби переробки інформації – система, послуга або інфраструктура, яка перетворює інформацію чи фізична локалізація, в якій знаходиться система.

Рекомендація – пояснення, що і як рекомендується зробити, щоб досягти цілей, визначених в політиках.

Третя сторона – це особа або орган, яка в разі вирішення проблеми, вважається незалежною від зацікавлених сторін.

Випадок, пов'язаний з безпекою інформації – є визначеним станом системи, послуги або мережі, який вказує на можливе порушення політики безпеки інформації, помилку забезпечення або невідому ситуацію, яка може бути пов'язана з безпекою.

Інцидент, пов'язаний з безпекою інформації - це є поодинокий випадок або серія небажаних чи несподіваних випадків, пов'язаних з безпекою інформації, що створює імовірність порушення дій і загрожує безпеці інформації

Загроза – потенційна причина небажаного інциденту, який може викликати шкоду в системі або організації.

Піддатливість – слабкість активу або групи активів, яка може бути використана щонайменше однією загрозою.

Ризик – комбінація імовірності випадку і його наслідку.

Аналіз ризику – систематичне використання інформації для ідентифікації джерел і оцінювання ризику.

Оцінювання ризику - процес співставлення оціненого ризику з визначеними критеріями з метою визначення значення ризику.

Оцінка ризику – цілісний процес аналізу та оцінювання ризику.

Акцептація (прийняття) ризику – рішення, щоб акцептувати (прийняти) ризик.

Поведінка з ризиком – процес вибору і впровадження модифікаційних засобів.

«Забезпечення» = «Засіб безпеки» = «Засіб захисту».

Залишковий ризик – ризик, що залишається після процесу дій з ризиком.

Управління ризиком – скоординовані дії керування і управління організацією з врахуванням ризику.

Забезпечення – засоби, що служать управлінню ризиком, разом з політиками, процедурами, рекомендаціями, організаційною практикою та структурами, які можуть мати адміністративну, технічну, юридичну природу або природу управління.

Декларація застосування (положення щодо застосування) - документ, в якому описано цілі застосування безпеки та забезпечення, які відносяться і мають застосування в СУІБ даної організації.

Цілі застосування безпек та забезпечення, додаток А до норми ДСТУ ISO/IEC 27001:2015, розділи від 5 до 15 є довідником, що містить найкращі практики, що стосуються безпек, визначених в А.5 до А.15.

V. Політика інформаційної безпеки у роботі виконкому Довгинцівської районної в місті Кривому Розі ради

Відповідно до Політики у сфері інформаційної безпеки в роботі виконкому Довгинцівської районної в місті ради і міжнародних стандартів: ДСТУ ISO/IEC 27001:2015 та ДСТУ ISO 9001:2015 ціллю впровадження системи управління інформаційною безпекою є забезпечення безпеки інформації, яка обробляється у виконкомі Довгинцівської районної в місті ради.

Для безпеки інформації в особистій сфері, а також безпеки матеріальних і нематеріальних активів здійснюються докладні заходи, для того щоб відповідати вимогам права, клієнтів та іншим вимогам, що випливають з умов.

Розпочаті процедурні дії базуються на знаннях про загрози та ризики у сфері інформаційної безпеки і дозволяють результативно керувати ними.

Беремо до уваги інформаційну безпеку шляхом управління власною і довіреною працівниками та клієнтами інформацією, а також управління ризиками в усіх аспектах доступності, інтегральності й секретності.

Систематично виконуємо заходи пов’язані з управлінням ризиками інформаційної безпеки на підставі прийнятої методики оцінки ризику та затверджених критеріїв оцінки, відносно виконання завдань у сферах управління, делегованих державою повноважень, виконання власних завдань органу місцевого самоврядування.

Захищаємо особисті дані працівників, громадян і клієнтів, які обробляються під час процесів надання послуг.

Захищаємо інформаційні активи для забезпечення безперервності надання послуг і виконання довірених завдань.

Керівництво виконкому забезпечує відповідальність працівників за реалізацію завдань у сфері виконання Політики у сфері інформаційної безпеки у роботі виконкому Довгинцівської районної в місті ради.

Політика у сфері інформаційної безпеки у роботі виконкому Довгинцівської районної в місті ради є головною політикою безпеки у роботі виконкому Довгинцівської районної в місті ради, у відношенні до політик зазначених в пунктах 1-11.

Координація дій у СУІБ покладається на уповноваженого з питань розробки та впровадження системи управління інформаційною безпекою.

1. Політика контролю доступу.

Виконком Довгинцівської районної в ради реалізовує політику контролю доступу у відношенні до зовнішніх сторін, клієнтів і працівників.

Клієнти мають визначений спосіб доступу до будівель виконкому, приміщень, інформації. Інформаційні системи, що використовуються, допомагають в обслуговуванні наших клієнтів і захищають інформацію відповідно до їх характеру.

У відношенні до зовнішніх сторін береться до уваги ряд чинників, які збільшують ризик порушення безпеки інформації і, як результат, використання засобів захисту.

Користувачі інформаційних систем у виконкомі Довгинцівської районної в місті ради діють згідно з визначеними принципами і методиками.

Контроль доступу відноситься до засобів обробки інформації в розумінні доступу:

- фізичного: робочі столи, шафи для документів, приміщення та інше;
- логічного: бази даних, інформаційні системи та інше;
- зв'язок між телеінформаційними мережами виконкому і третьою стороною, як постійний зв'язок, віддалений доступ;
- на місці, тобто в об'єктах виконкому або поза локалізацією виконкому.

Працівники мають доступ до призначених комп'ютерів і програм комп'ютерного захисту шляхом використання ідентифікатора (застосування уповноважень і паролів).

Відповідно до прийнятої класифікації інформації до конфіденційної та таємної інформації можуть мати доступ лише визначені особи.

Нагляд за доступом проводиться через призначення осіб, які діють від імені керівництва виконкому.

2. Політика використання програмного забезпечення.

Для охорони інформації і програмного забезпечення, а також з метою уникнення порушень норм права, виконком Довгинцівської районної в місті ради забороняє використання неавторизованого програмного забезпечення.

Будь-яке програмне забезпечення, що інсталюється в комп'ютерах, повинне встановлюватись із згодою визначеної особи, яка авторизує програмне забезпечення.

3. Політика захисту від ризиків.

Для реалізації заходів обережності, щодо запобігання і виявлення потрапляння шкідливого програмного забезпечення, такого як віруси, комп'ютерні черв'яки, трояни, логічні бомби, на комп'ютерах виконкому інсталюються антивірусні програми для запобігання, виявлення й усунення шкідливого коду, а також нагляду за мобільним кодом.

Антивірусне програмне забезпечення повинно бути авторизоване визначеною особою.

Програмне забезпечення має постійно та систематично оновлюватись.

Обов'язками користувача комп'ютера є:

- перевірка всіх файлів на електронних або оптичних носіях, а також файлів одержаних через мережу на наявність шкідливого коду;
- перевірка вкладень електронної пошти, а також завантажених даних на наявність шкідливого коду.

Застосування програмного забезпечення такого як: комунікатори, Java-засоби, яке може бути носієм мобільного коду, повинно бути авторизоване. Перед застосуванням програмного забезпечення цього типу необхідно отримати згоду працівника визначеного керуючим справами.

4. Політика обміну інформацією.

Політика обміну інформацією базується на нормативних вимогах. Обмін інформацією повинен проводитися способом, який захищений відповідно до потреб, що обумовлені класифікацією інформації, а також дотримується авторського права.

Працівники, виконавці та інші споживачі зобов'язані не діяти на шкоду виконкому.

5. Політика захисту інформації пов'язана із сполученням між бізнесовими інформаційними системами.

Використання сполучення між бізнесовими інформаційними системами реалізується на основі раніше проведеної оцінки ризику.

Офісні системи документообігу забезпечують захист інформації при використанні: документів, комп'ютерів, мобільної обробки, мобільного зв'язку, пошти, голосової пошти, мультимедійних засобів, поштових послуг, а також факсів.

Працівники застосовують відповідні принципи, пов'язані із захистом інформації.

6. Політика чистого робочого столу і чистого екрану.

Для обмеження ризику неавторизованого доступу, втрати або ушкодження інформації під час роботи і поза годинами роботи, застосовується політика чистого робочого столу для паперових документів і носіїв даних, а також політика чистого екрану для засобів обробки інформації. Працівники застосовують відповідні принципи пов'язані з політикою чистого робочого столу і чистого екрану відповідно до характеру інформації, згідно з класифікацією.

7. Політика користування мережевими послугами.

Користування мережею і мережевими послугами, користувачами відбувається на підставі їх авторизації в мережі. Нагляд за доступом до мережі і мережних послуг проводиться визначеними особами, які діють від імені керівництва виконкому.

8. Політика віддаленої роботи.

Керівництво виконкому допускає роботу на відстані при застосуванні відповідних засобів захисту. Робота на відстані може проводитись на підставі уповноваження зі сторони керівництва виконкому. Умови роботи зобов'язані забезпечити відповідну фізичну і логічну охорону інформаційних активів. Докладні умови роботи будуть описані в окремих документах.

9. Політика дотримання авторського права.

Виконавчий комітет Довгинцівської районної в місті Кривому Розі ради направляє свої дії на захист авторських прав. Використання програмного забезпечення і інформації повинне проводитися згідно з державним і міжнародним правом.

У випадках порушення авторського права працівниками виконкому до них будуть застосовуватися дисциплінарні стягнення.

10. Політика захисту особистих даних і приватності.

Виконавчий комітет Довгинцівської районної в місті Кривому Розі ради реалізує захист особистих даних і приватності у відношенні до працівників,

мешканців міста, клієнтів та інших фізичних та юридичних осіб. Для забезпечення захисту особистих даних і приватності визначаються відповідні засоби, які будуть здійснювати нагляд за їх збереженням. Контроль у сфері здійснення захисту особистих даних або приватності фізичних осіб здійснюють керівники структурних підрозділів.

11. Політика використання криптографічних засобів захисту.

З метою захисту вразливої інформації у виконкомі застосовуються криптографічні засоби захисту.

Для надання можливості використання криптографічної техніки, здійснюється управління ключами, щоб всі ключі були захищені від модифікації, втрати або знищення.

VI. Принципи інформаційної безпеки.

Принципи інформаційної безпеки, що застосовуються у виконкомі докладно регулюють політику інформаційної безпеки.

1. Основні принципи безпеки людських ресурсів

Угоди з працівниками, виконавцями, споживачами, які представляють треті сторони, повинні містити підписані принципи і умови надання роботи.

1.1 Перед наданням роботи:

1.1.1 Посадова інструкція;

1.1.2 Процедура перевірки;

1.1.3 Принципи і умови надання роботи.

1.2 Під час надання роботи:

1.2.1 Відповідальність керівництва;

1.2.2 Удосконалення і навчання;

1.2.3 Дисциплінарні процедури.

1.3 Закінчення або зміна роботи:

1.3.1 Відповідальність, пов’язана із закінченням роботи;

1.3.2 Повернення активів;

1.3.3 Позбавлення прав доступу.

2. Принципи реєстрації інцидентів інформаційної безпеки.

У випадку порушення інформаційної безпеки, потрібно якнайшвидше повідомити про інцидент головного спеціаліста з питань інформаційних технологій та програмного забезпечення.

Всі працівники і користувачі сторонніх організацій, які користуються інформаційними системами та послугами, повинні якнайшвидше повідомити про будь-які виявлені порушення безпеки в системах чи послугах головного спеціаліста з питань інформаційних технологій та програмного забезпечення.

3. Принципи роботи з носіями даних.

3.1 Управління носіями даних.

Для керування носіями інформації повинні існувати відповідні процедури, а саме:

3.1.1 Забезпечення збереження інформації.

3.1.2 Забезпечення антивірусного захисту.

3.1.3 Перевірка програм та файлів антивірусною програмою.

3.1.4 Унеможливлення викрадення носія з даними.

3.2 Утилізація носіїв інформації (коли вичерпано ресурси носія інформації він повинен бути надійно і безпечно утилізований за допомогою певних процедур).

3.3 Носії даних повинні бути застосовані лише для цілей пов'язаних з роботою виконкому.

3.4 Винесення носія з даними за межі адміністративної будівлі районної в місті ради має здійснюватись на підставі отриманого дозволу від керівника структурного підрозділу, якому підпорядкований працівник.

4. Принципи використання робочих станцій, електронної пошти та Інтернету.

Використання робочих станцій працівниками виконкому залежить від характеру роботи, яка виконується. Відповідно до цього на робочій станції встановлено відповідне програмне забезпечення та антивірусний захист. Отримані програми та файли електронною поштою необхідно перевіряти антивірусною програмою.

Після завершення робочого часу працівник зобов'язаний вимкну-ти комп'ютер та периферійні пристрої. Якщо працівник ненадовго залишає робоче місце, він зобов'язаний заблокувати комп'ютер, щоб унеможливити несанкціоноване використання робочої станції під час відсутності працівника. Електронна пошта є одним з елементів колективної роботи працівників виконкому і незамінним інструментом обміну інформацією. Несанкціонований доступ до поштової скриньки працівника неможливий завдяки блокуванню комп'ютера.

5. Принципи роботи з даними в паперовій і електронній формі.

5.1 Важливі облікові записи організації повинні бути захищені від втрати, пошкодження та фальсифікації відповідно до вимог, встановлених чинним законодавством, рішеннями Довгинцівської районної в місті Кривому Розі ради та її виконавчого комітету, розпорядженнями голови районної в місті ради.

5.2 Дані не можуть бути переказані іншим особам, які не пов'язані з процесами виконання обов'язків у виконкомі без дозволу керівника.

5.3 Дані у паперовому вигляді повинні бути надійно захищені в шафах та офісних столах, відповідно до їх класифікації.

5.4 Дані в електронному та паперовому вигляді, що містять інформацію про працівників, клієнтів, та інших осіб, які обслуговуються працівниками виконкому органів повинні бути надійно захищені, як конфіденційна інформація.

6. Принципи використання переносних комп'ютерів.

Переносні комп'ютери, в яких знаходяться інформаційні дані, повинні бути захищені власником активу. Використання комп'ютера та його виніс можливий після отримання дозволу від керівника або відповідальної особи.

7. Принципи використання засобів обробки інформації поза адмінбудівлею, а також винесення майна.

Використання засобів переробки інформації поза межами організації має бути авторизоване керівництвом, незалежно від того, хто є їх власником.

У відношенні до охорони пристроїв, які знаходяться поза адмінбудівлею виконкому:

- не залишати в публічних місцях без нагляду пристроїв або носіїв, які виносяться за межі адмінбудівлі виконкому; перевозити переносні комп'ютери, як ручний багаж і в міру можливості, маскувати їх під час подорожі;
- дотримуватися інструкцій виробника стосовно охорони пристроїв (напр. охорони перед виставленням на сильні електромагнітні поля);
- застосовувати відповідні забезпечення, визначені в процесі оцінювання ризику, необхідні під час праці вдома (напр. закривання шафки, політика чистого офісу, забезпечення доступу до комп'ютерів та безпечне з'єднання з офісом);
- гарантувати відповідне збереження пристроїв, які використовуються поза адмінбудівлею виконкому.

Забороняється виносити пристрої, інформацію або програми без попереднього дозволу.

8. Принципи використання паролів і збереження таємниці.

8.1 Надання паролів контролюється, таким чином:

- підписання користувачами зобов'язання щодо зберігання таємниці особистих паролів та паролів робочих груп, до яких вони належать;
- забезпечення постачання нових, тимчасових або замінних паролів після попереднього підтвердження тотожності користувача;
- безпечний спосіб видання користувачам тимчасових паролів; необхідно уникати посередництва інших осіб або використання незахищених повідомлень електронної пошти (які присилаються так званим відкритим текстом);
- унікальність тимчасових паролів для користувачів і складність їх розшифрування;
- підтвердження отримання паролів користувачами;
- заборона зберігання паролів в незахищеному вигляді в комп'ютерних системах;
- необхідність зміни передбачуваних паролів, наданих виробником під час інсталяції системи або програмного забезпечення.

8.2 Під час обрання і використання паролів, користувачі мають дотримуватись правил згідно з перевіреними практиками безпеки. Користувачі повинні:

- зберігати паролі в секреті;
- уникати записування паролів (наприклад на папері, в файлі або переносному пристрої); паролі можна записувати тільки у випадку, якщо вони зберігаються в безпечному місці, а їх спосіб зберігання підтверджений;
- негайно змінювати паролі у випадках, коли будь-що вказує на можливість порушення безпеки системи чи паролю;
- вибирати якісні паролі з достатньо мінімальною довжиною які:

- можна легко запам’ятати;

- не основані на простих асоціаціях, які легко вгадати чи зробити висновки з інформації, яка стосується даної особи, наприклад імена, номери телефонів, дати народження і т.д.;

- не піддатливі на словникову атаку (це означає, що не містять вони слів із словників);

- не містять ряду однакових знаків або груп знаків, які складаються тільки з цифр або тільки з літер;

- змінювати паролі в регулярних інтервалах часу або після визначеної кількості реєстрацій в системі (рекомендується, щоб паролі привілейованих рахунків мінялися частіше інших паролів) і уникати повторення паролів чи „циклічного” вживання старих паролів;

- змінювати тимчасові паролі під час першого входження до системи;

- не вводити паролів до будь-яких автоматизованих процесів входження до системи, наприклад не переховувати їх в макросах і не приписувати до функціональних клавіш;

- не надавати доступу до своїх паролів іншим користувачам;

- не використовувати однакових паролів для використання у роботі і поза нею.

9. Принципи доступу зовнішніх сторін до засобів перетворення інформацій.

Доступ зовнішніх сторін до засобів перетворення інформацій, що не залежать від організації, для перетворення і передачі інформації контролюється визначеними особами.

Під час доступу зовнішніх сторін до засобів перетворення інформацій потрібно взяти до уваги:

- засоби перетворення інформацій, до яких можуть мати доступ зовнішні сторони;

- спосіб доступу зовнішньої сторони до інформації та засобів пере-творення, інформації наприклад:

- доступ фізичний (наприклад до офісу, комп’ютерного залу, шаф);

- доступ логічний (наприклад до баз даних організації, інформаційних систем);

- зв’язок між мережами організації та зовнішніх сторін (наприклад зв’язок постійний, доступ віддалений);

- доступ є на місці, чи поза межами організації;

- вартість та вразливість доступної інформації і критичність для процесів виконкому;

- забезпечень необхідних для охорони інформації, які в основі є недоступними зовнішнім сторонам;

- персонал зовнішньої сторони, який обслуговує інформацію, що належить організації;

- спосіб визначення організації та персоналу, що має доступ, перевірки прав та частоти підтвердження цих потреб;

- різних засобів та забезпечення впровадженого зовнішньою стороною для зберігання, передавання, співкористування та обміну інформації;

- результати браку доступу зовнішньої сторони, коли він вимагається та впровадження або отримання невиправних інформацій або таких, що вводять в помилки;

- практики та процедури обслуговування інцидентів пов'язаних з безпечністю інформації та потенційної шкоди, також підстав та умов підтримування безперервності доступу зовнішньої сторони у випадку виникнення інциденту пов'язаного з безпечністю інформації;

- правові вимоги, внутрішні регулювання та інші договірні зобов'язання, властиві для зовнішньої сторони, які пропонується взяти до уваги.

10. Принципи обробки інформації та обміну інформацією.

10.1 Реагування, обробка, зберігання та переказування інформації, повинно проходити згідно з її класифікацією. Необхідно керуватись такими принципами:

- обслуговування та позначення всіх носіїв, згідно з рівнем їх класифікації;
- обмеження доступу, яке запобігає несанкціонованому доступу персоналу;
- дотримання формального реєстру авторизованих одержувачів інформації;
- забезпечення правильної обробки вихідних даних і правдивості вхідних даних;
- захист непереданих даних згідно з їх рівнем конфіденційності;
- зберігання носіїв згідно із специфікаціями виробника;
- обмеження розповсюдження даних до мінімуму;
- зрозуміле позначення всіх копій носія для авторизованих одержувачів;
- регулярний перегляд списків дистриб'юторів та авторизованих одержувачів.

10.2 Обмін інформацією, при використанні електронних комунікаційних засобів повинна враховувати:

- захист інформації, якою обмінюються від перехоплення, копіювання, модифікації, помилкової маршрутизації та знищення;
- виявлення та захист від шкідливих програм, які можуть пересилатися за допомогою використання електронних засобів комунікації;
- захист конфіденційної електронної інформації, яка передається у формі додатків;
- рекомендації, які визначають затверджений спосіб використання електронних комунікаційних пристроїв;
- використання безпровідної комунікації з урахуванням особливих ризиків, які з нею пов'язані;
- працівників, виконавців та всіх інших користувачів щодо не завдавання шкоди організації, наприклад наклеп, нарікання, удавання, пересилання ланцюгових листів, несанкціоновані закупівлі і т.д.;
- використання криптографічних технік, наприклад, для захисту конфіденційності, інтегральності та достовірності інформації;

- рекомендації щодо зберігання та знищення повідомлень і кореспонденції, відповідно до законодавства та внутрішніх документів;
- заборону залишати листи, доповідні, пояснювальні, що містять конфіденційну інформацію поруч з друкарською технікою: принтерами, копіювальними апаратами, факсами, до яких може мати доступ не уповноважений персонал;
- забезпечення та обмеження пов'язані з пересиланням повідомлень за допомогою засобів комунікації, наприклад автоматична пере-адресація електронної пошти назовні;
- застосування відповідних засобів безпеки, наприклад під час розмов телефоном не розголошувати конфіденційну інформацію.

Уникати підслуховування або перехоплення:

- особами, які знаходяться безпосередньо близько, якщо використовуються мобільні телефони;
- застосування різноманітних засобів підслуховування, фізичний доступ до слухавки, телефонної лінії або скануючих пристроїв;
- особами, які знаходяться на стороні співрозмовника;
- неможливість залишати повідомлення, які містять конфіденційну інформацію, на автовідповідачах, тому що вони можуть прослуховуватись не уповноваженими особами або невідповідно записаними внаслідок помилки в наборі номеру;
- навчання персоналу щодо проблем, які виникають при використанні факсів:
- можливість несанкціонованого доступу до вбудованої пам'яті з метою отримання інформації;
- навмисне або випадкове програмування факсів таким чином, що повідомлення будуть висилатись на визначені номери;
- відправлення документів чи повідомлень на неправильний номер внаслідок помилки в наборі номеру або використання невідповідного номеру з пам'яті пристрою;
- в жодному програмному забезпеченні не залишати адреси електронної пошти або іншої особистої інформації, яка може збиратися з метою несанкціонованого використання;
- факс-модеми та сканери на випадок помилок в трансмісії зберігають сторінки в пам'яті і друкують їх одразу після усунення помилки;
- конфіденційні розмови не можуть вестися в публічних місцях, відкритих бюро або місцях зустрічей, де відсутня звукоізоляція;
- засоби обміну інформацією мають відповідати відповідним юридичним вимогам.

10.3 З метою обміну інформацією та програмним забезпеченням між організацією та зовнішніми сторонами, рекомендується укладання угод щодо обміну інформацією.

10.4 Повинен бути забезпечений захист носіїв, які містять інформацію, від несанкціонованого доступу, невідповідного використанням чи пошкодженням під час транспортування за межі організації.

11. Принципи прийняття третіх осіб в приміщеннях виконкому:

- персонал має знати сфери існування безпечної території та ведення в ній діяльності;
- уникнення виконання роботи без нагляду на безпечній території з огляду на безпечність та унеможливити шкідливу діяльність;
- замкнення та періодична перевірка безпечної території, де немає людей;
- не допускати користуватися пристроями фотографування, відео-, аудіо- або інших записних пристроїв, напр. мобільних камер за винятком, коли особа має відповідне уповноваження.

12. Принципи охорони устаткування і залишення місця роботи.

12.1 Користувачі повинні забезпечувати відповідний захист обладнання залишеного без нагляду:

- вимкнення терміналу після закінчення роботи, крім випадків коли вони забезпечені відповідною системою, що блокує доступ, наприклад вимикач екрану захищений паролем;
- вихід з комп'ютерної системи класу "mainframe", серверів, офісних комп'ютерів в момент закінчення сесії (а не тільки вимикати монітор чи термінал);
- забезпечення особистих комп'ютерів чи терміналів, які не використовуються в даний момент від несанкціонованого доступу за допомогою блокування клавіатури чи іншим рівноцінним способом, наприклад доступ до комп'ютера після введення паролю.

12.2 Для впровадження політики чистого столу для паперової документації та носіїв, а для засобів обробки інформації - політики чистого екрану, працівники повинні:

- зберігати під замком (найкращим засобом є сейф, шафа або інша форма збереження) конфіденційну інформацію організації, яка не використовується, наприклад розміщених на електронних носіях або у вигляді паперових документів, особливо якщо приміщення залишається без нагляду;
- закривати сесії або блокувати комп'ютери чи термінали, залишені без нагляду або такі, що тимчасово не використовуються (за допомогою механізму блокування екрану і клавіатури контрольованим паролем, детектору або іншого подібного механізму);
- захищати пункти отримування і висилання кореспонденції та неконтрольовані факси;
- забороняти використання ксероксів або іншої копіювальної техніки (наприклад сканерів, цифрових апаратів) без авторизації;
- негайно усувати з принтерів документи, які містять конфіденційну інформацію.

13. Принципи поводження з ключами від приміщень, а також канцелярських шаф.

Ключі від приміщень повинні бути збереженні. За ключі від приміщень повинні відповідати визначені керівником особи тобто:

- приміщення, які відносять до безпечної зони – ключі знаходяться у відповідальних працівників, які там працюють. Прибирання здійснюється у присутності працівників відділу.
- приміщення голови районної в місті ради – ключі у голови районної в місті ради та секретаря. Прибирання здійснюється в присутності секретаря.
- приміщення заступників голови районної в місті ради та керуючого справами виконкому – ключі у заступника, керуючого справами виконкому та секретаря. Прибирання здійснюється в присутності секретаря.
- приміщення структурних підрозділів виконкому – ключі у відповідального чергового.
- канцелярські шафи – ключі у відповідальних працівників.

14. Реєстрація змін у документації.

Кожен працівник має право внести пропозицію щодо зміни до документації. Про свою пропозицію інформує свого керівника. Рішення щодо запропонованих змін приймається на засіданні робочої групи з питань розробки та впровадження системи управління інформаційною безпекою виконкому районної в місті ради.

15. Принципи класифікації інформації.

Принципи класифікації інформації записано в регулюючому документі «Методика управління ризиками», та розповсюджуються, зокрема, на такі види інформації:

- відкрита інформація;
- конфіденційна інформація;
- таємна інформація.

Принципи класифікації інформації регулює закон України «Про державну таємницю».

Керуючий справами виконкому ***Олександр Гижко***

Додаток 3
до розпорядження голови
районної в місті ради
від 24.11.2021 № 345-р

План
зниження ризиків системи управління інформаційною безпекою у виконкомі Довгинцівської районної в місті ради

№ з/п	*Ризик*	*Уразливість*	*Заходи по обробці ризику*	*Дата*	*Коментарі, ресурси, відповідальні особи у виконкомі районної в місті ради*
Імідж та репутація					
1	Розголошення, порушення цілісності та обмеження доступу до службової інформації	Відсутність інформування персоналу про статус службової інформації, на документах якої проставляється гриф «Для службового користування»	Організувати оперативне інформування персоналу про статус службової інформації, на документах якої проставляється гриф «Для службового користування», виконувати маркування інформації	Постійно	Структурні підрозділи та галузеві спеціалісти
2	Порушення вимог ІБ через невчасну актуалізація таких вимог	Відсутність інформування персоналу про загрози інформаційної безпеки	Організувати аналіз та оперативне інформування персоналу про можливі загрози інформаційної безпеки	Щоквартально	Структурні підрозділи та галузеві спеціалісти
Вебсайт виконкому					
3	Втрата доступу до сайту та порушення цілісності інформації	Вірусна атака Відсутність або недостатність антивірусного	Проаналізувати ступінь захищеності вебсерверу, на якому розміщується сайт виконкому, при необхідності перенести сайт на	Постійно	Відділ інформаційних технологій

№ з/п	*Ризик*	*Уразливість*	*Заходи по обробці ризику*	*Дата*	*Коментарі, ресурси, відповідальні особи у виконкомі районної в місті ради*
	внаслідок хакерської атаки	захисту	більш захищений сервер Переглянути склад осіб, що мають доступ до технологічної інформації сайту		
Документи номенклатури справ виконкому та структурних підрозділів виконкому районної в місті ради					
4	Втрата інформації в разі виникнення пожежі або інших надзвичайних ситуацій	Пожежа у службових приміщеннях виконкому, пошкодження архіву внаслідок виникнення надзвичайних ситуацій Відсутність протипожежних засобів	Проведення інструктажу з правилами поводження при виникненні пожежі та надзвичайних ситуацій	Раз на рік	Відділ з питань мобілізаційної роботи, надзвичайних ситуацій та цивільного захисту населення, завідувач господарства
5	Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними	Втрата інформації при тимчасовій відсутності працівника або в раз звільнення	Проведення навчань у відділах за різними напрямками діяльності. Забезпечення передачі досвіду та повного обсягу інформації іншим спеціалісту (спеціалістам) у разі звільнення працівника з посади Проводити контроль дій персоналу стосовно поводження із документами (зберігання, переміщення, видалення)	У разі потреби, при звільненнях або переведеннях	Структурні підрозділи та галузеві спеціалісти
6	Псування документів через вплив на них факторів навколишнього середовища.	Зберігання документів у місцях, де є прямий доступ сонячного світла та рівень вологості повітря	Не зберігати документи на підвіконнях, використовувати захисні покриття на вікнах де зберігаються документи. Якщо документи не зберігаються у спеціально виділених	Постійно	Структурні підрозділи та галузеві спеціалісти

№ з/п	*Ризик*	*Уразливість*	*Заходи по обробці ризику*	*Дата*	*Коментарі, ресурси, відповідальні особи у виконкомі районної в місті ради*
		не перебуває у межах норми	приміщеннях (архівних приміщеннях), то повинні бути захищені від прямих сонячних променів. Дослідити рівень впливу зовнішніх факторів на збереження документів.		
7	Порушення конфіденційності або втрата документів через доступність третіх осіб до приміщення кабінету	Вільний доступ до приміщень в робочий час. Розповсюдження службової інформації, на документах якої проставляється гриф «Для службового користування» через втрату документів. Втрата або розповсюдження службової інформації, на документах якої проставляється гриф «Для службового користування» внаслідок порушення Регламенту виконкому районної в місті ради, порядку доступу до приміщень	Здійснити позапланові перевірки дотримання порядку доступу до приміщень виконкому Організувати вивчення Регламенту виконкому районної в місті ради щодо порядку поводження зі службовими документами. Визначити зони вільного доступу до приміщень та зон з обмеженим доступом (навіть в межах окремого приміщення). Поінформувати відповідальний персонал про режими доступу до приміщень виконкому.	Постійно	Відділи: інформаційних технологій, загальний
8	Неконтрольоване розповсюдження інформації співробітниками	Несанкціоноване копіювання або розповсюдження інформації	Встановити та інформувати співробітників про службову інформацію, на документах якої проставляється гриф «Для службового користування» та правила розповсюдження	Постійно	Члени робочої групи з питань розробки та впровадження

№ з/п	*Ризик*	*Уразливість*	*Заходи по обробці ризику*	*Дата*	*Коментарі, ресурси, відповідальні особи у виконкомі районної в місті ради*
			такої інформації. Розмістити та користуватися копіювальними пристроями таким чином, щоб попередити несанкціоноване копіювання документів, на яких проставлений гриф «Для службового користування».		СУІБ Структурні підрозділи та галузеві спеціалісти
Спеціальне програмне забезпечення (1С-бухгалтерія , Програма в системі ЕГСКП від Нова-Ком, M.E.DOC (програма звітності до податкової інспекції та пенсійного фонду), Клієнт-банк, Інформаційна система «Картка» , Єдина інформаційна система «Діти»					
9	Втрата інформації внаслідок виходу зі строю апаратної частини робочої станції.	Вихід зі строю апаратної частини робочої станції в наслідок перебоїв у електромережі	Забезпечення пристроями безперебійного живлення всі персональні комп'ютери, на яких встановлено спеціальне програмне забезпечення або інформаційні системи. Дослідити надійність апаратної частини робочих станцій та за можливості передбачити їх модернізацію або заміну на більш надійні.	Постійно	Відділ інформаційних технологій
Персонал					
10	Втрата або витік службової інформації через дії третіх осіб	Витік службової інформації, на документах якої проставляється гриф «Для службового користування» через дії осіб, що залучаються для сервісного обслуговування засобів обробки інформації, програмних продуктів	Доступ до приміщень де зберігається службова інформації, на документах якої проставляється гриф «Для службового користування» третім особам надавати лише після впровадження відповідних заходів безпеки. Здійснення контролю щодо недопущення витоку службової інформації, на документах якої проставляється гриф «Для службового	У разі необхідності	Члени робочої групи з питань розробки та впровадження СУІБ Структурні підрозділи та галузеві спеціалісти

№ з/п	*Ризик*	*Уразливість*	*Заходи по обробці ризику*	*Дата*	*Коментарі, ресурси, відповідальні особи у виконкомі районної в місті ради*
			користування» під час сервісного обслуговування засобів обробки інформації, програмних продуктів сторонніми організаціями. Передбачити наявність в договорах (угодах) із третіми особами вимог по забезпеченню інформаційної безпеки.		
11	Часткова або значна втрата через розголошення службової інформації під час роботи та після звільнення.	Розголошення службової інформації, на документах якої проставляється гриф «Для службового користування» працівниками після звільнення з роботи	Запровадити підписання працівникам під час звільнення з роботи зобов'язання щодо захисту персональних даних та збереження інформації з обмеженим доступом (протягом узгодженого проміжку часу)	У разі необхідності	Відділ з питань кадрової роботи
Робочі станції					
12	Втрата інформації внаслідок ураження комп'ютерними вірусами або реалізації хакерської атаки	Вірусна атака Відсутність або недостатність антивірусного захисту	Забезпечення оновлення антивірусних баз даних Проводити перевірку роботи антивірусного програмного забезпечення та засобів захисту від хакерських атак	Постійно	Відділ інформаційних технологій
13	Припинення роботи обладнання через відключення живлення та внаслідок аварій засобів життєзабезпечення.	Відключення живлення внаслідок аварій	Забезпечення пристроями безперебійного живлення Дослідити можливість облаштування резервними джерелами живлення	Постійно	Відділ інформаційних технологій

№ з/п	*Ризик*	*Уразливість*	*Заходи по обробці ризику*	*Дата*	*Коментарі, ресурси, відповідальні особи у виконкомі районної в місті ради*
Електронний документообіг					
14	Неконтрольоване розповсюдження інформації співробітниками	Несанкціоноване копіювання або розповсюдження інформації	Встановити та інформувати співробітників про службову інформацію, на документах якої проставляється гриф «Для службового користування» та правила розповсюдження такої інформації. Видаляти або переносити на захищені носії інформації електроні документи, які містять службову інформацію, на документах якої проставляється гриф «Для службового користування», але які більше не потрібні в роботі. При звільненні або переведенні працівників контролювати збереження всіх електронних документів, які були доступні цим працівникам. Розмістити та користуватися копіювальними пристроями таким чином, щоб попередити несанкціоноване копіювання службової інформації, на документах якої проставляється гриф «Для службового користування»	Постійно	Члени робочої групи з питань розробки та впровадження СУІБ Структурні підрозділи та галузеві спеціалісти
Приміщення					

№ з/п	*Ризик*	*Уразливість*	*Заходи по обробці ризику*	*Дата*	*Коментарі, ресурси, відповідальні особи у виконкомі районної в місті ради*
15	Втрата інформації в разі виникнення пожежі або інших надзвичайних ситуацій	Пожежа у службових приміщеннях виконкому Відсутність засобів пожежогасіння, попередження про пожежі або надзвичайній ситуації	Дотримання вимог інструктажів з пожежної безпеки	Щоквартально	Завідувач господарства
16	Втрата інформації через несанкціонованого підключення до мереж	Відкритий доступ до кабельної мережі	Захистити кабельні мережі	У разі необхідності	Завідувач господарства, відділ інформаційних технологій
17	Втрата інформації через пошкодження обладнання в наслідок несанкціонованого відключення живлення	Відкриті розподільчі щитки	Опломбувати розподільчі щитки. Впровадити дисциплінарні процедури стосовно порушення вимог доступу до щитків	У разі необхідності	Завідувач господарства

Керуючий справами виконкому ***Олександр Гижко***

Додаток 4
до розпорядження голови
районної в місті ради
від 24.11.2021 № 345-р

Методика
виявлення та реєстрації інцидентів інформаційної безпеки
у виконкомі Довгинцівської районної в місті ради

Зміст

1. Вступ

Методика виявлення та реєстрації інцидентів інформаційної безпеки у виконкомі Довгинцівської районної в місті ради (далі - методика виявлення та реєстрації інцидентів) розроблена відповідно до вимог ДСТУ ISO/IEC 27001:2015 та розповсюджується на всі структурні підрозділи виконкому районної в місті ради.

Цілі впровадження методики виявлення та реєстрації інцидентів:

- оперативний моніторинг стану інформаційної безпеки в рамках дії системи інформаційної безпеки виконкому районної у місті ради;
- виявлення, облік, реагування, розслідування та аналіз інцидентів інформаційної безпеки;
- інформування керівництва виконкому районної в місті ради та зацікавлених осіб про поточний стан інформаційної безпеки.

При здійсненні дій пов’язаних із управлінням інцидентами керуватися даною методикою, а також настановами актуальними стандартами ISO/IEC 27001 та ISO/IEC 27002 (його національними версіями, або іншим нормативним документом, що їх замінюють).

Вимоги методики розповсюджуються на всі структурні підрозділи виконавчого комітету районної в місті ради.

Відповідальність за управління інцидентами, а також за контролювання

дотримання вимогам даного положення несе керуючий справами виконкому Довгинцівської районної в місті ради.

2. Терміни та визначення

В даному положенні використовуються терміни та визначення понять згідно ДСТУ ISO/IEC 27001:2015 та ISO/IEC 27002:2013, а також такі:

Подія інформаційної безпеки - ідентифікований випадок стану системи або мережі, який вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту, або раніше невідома ситуація, яка може бути істотною для безпеки.

Інцидент інформаційної безпеки - подія, що є наслідком одного або декількох небажаних або несподіваних подій ІБ, що мають значну ймовірність компрометації операції і створення загрози ІБ.

Група реагування на інциденти інформаційної безпеки (ГРІІБ) являється групою (командою) відповідно навчених працівників виконкому районної в місті ради, яка обробляє інциденти ІБ під час їхнього життєвого циклу. Іноді ця група може доповнюватися зовнішніми експертами, наприклад, з офіційно визнаною групи реагування на комп'ютер-ні інциденти або комп'ютерної групи швидкого реагування (КГШР).

Хост (вузол) - будь-який пристрій, що надає сервіси формату «клієнт-сервер» в режимі сервера з будь-якими інтерфейсам і унікально визначене на цих інтерфейсах;

Додаток (застосунок, застосовна програма, прикладна програма) - користувацька комп'ютерна програма, що дає змогу вирішувати конкретні прикладні задачі користувача;

Експлой - комп'ютерна програма, фрагмент програмного коду або послідовність команд, що використовують вразливості в програмному забезпеченні та призначені для проведення атаки на обчислювальну систему.

3. Нормативні посилання

В даній методиці використовуються посилання на наступні нормативні документи:

- ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги»;
- ISO/IEC 27002:2013 «Інформаційні технології. Методи забезпечення безпеки. Звід правил по управлінню захистом інформації».

4. Предмет методики та опис дій

4.1. Ознаки інциденту інформаційної безпеки

Припущення того, що в виконкомі районної в місті ради стався інцидент інформаційної безпеки, має базуватися на трьох основних факторах:

- повідомлення про інцидент інформаційної безпеки надходять одночасно з декількох джерел (працівники виконкому, системи виявлення вторгнення (IDS), журнальні файли);

- IDS сигналізують про багаторазове повторення подій;
- аналіз журнальних файлів автоматизованої системи дає підставу для висновку про можливість настання події інциденту.

В загальному випадку, ознаки інциденту поділяються на дві основні категорії, повідомлення про те, що інцидент відбувається в да-ний момент і повідомлення про те, що інцидент, можливо, відбудеться в недалекому майбутньому. Нижче перераховані деякі ознаки здійснюваної події:

- IDS фіксує переповнення буферу;
- повідомлення антивірусної програми;
- крах web-інтерфейсу;
- працівники виконкому повідомляють про достатньо низьку швидкість при спробі виходу в Internet;
- посадова особа виконкому, на яку відповідно до розподілу обов'язків покладені обов'язки системного адміністратора фіксує наявність файлів з підозрілими назвами;
- працівники виконкому повідомляють про наявність у своїх поштових скриньках багатьох повторюваних повідомлень;
- хост (вузол) вносить запис до журналу аудиту про зміну конфігурації;
- додаток фіксує в журнальному файлі множинні невдалі спроби авторизації;
- посадова особа виконкому, на яку відповідно до розподілу обов'язків покладені обов'язки адміністратора мережі фіксує різке збільшення мережевого трафіку.

Прикладами подій, які можуть стати джерелами інформаційної безпеки можуть бути:

- журнальні файли сервера, які фіксують сканування портів;
- оголошення про появу нового виду експлойту;
- відкрита заява комп'ютерних злочинців про наміри організації та інше.

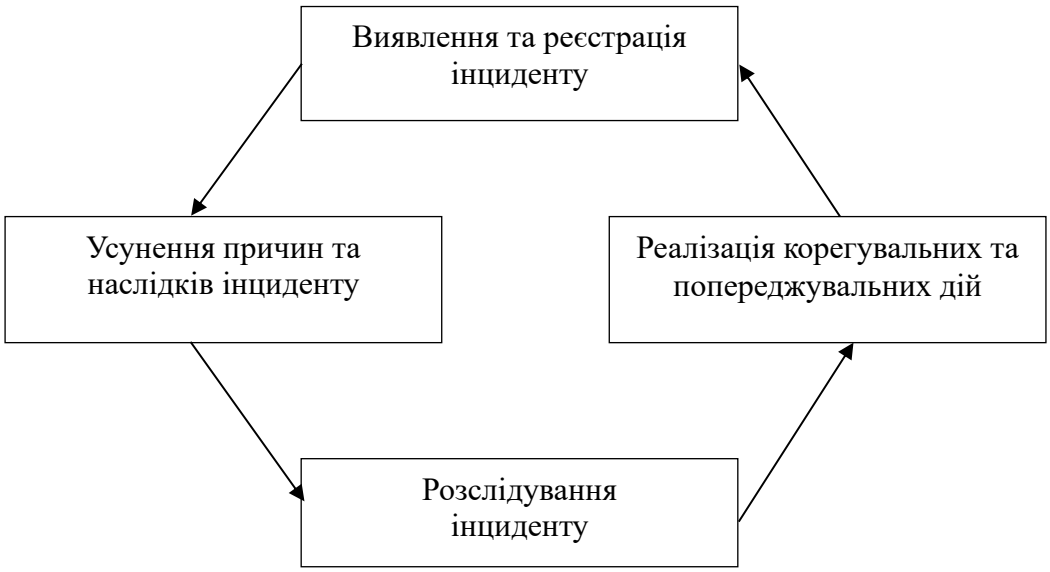
4.2. Виявлення і реєстрація інциденту

Інцидент інформаційної безпеки може помітити працівник виконкому або посадова особа виконкому відповідальна за функціонування системи управління інформаційною безпекою. Для працівників виконкому районної в місті ради має розроблятися інструкція, яка буде містити опис, в якому вигляді співробітник повинен повідомити про виникнення інциденту, координати відповідальних осіб, а також перелік дій, які співробітник може виконати самостійно (або попередити про те, що виконувати які-небудь дії самостійно заборонено). Такий звіт повинен містити докладний опис інциденту, перелік співробітників, залучених до інциденту, прізвище співробітника, що зафіксував інцидент та дату виникнення і реєстрації інциденту. Також повинні бути вказані дії для фахівця, до обов'язків якого входить реєстрація інциденту. Співробітник, що знайшов інцидент, зв'язується із співробітником, відповідальним за реєстрацію інциденту для виконання подальших дій. Також співробітники можуть звернутися напряму до фахівця, який може усунути наслідки й причини інциденту (наприклад, до посадової особи виконкому відповідальної за функціонування системи управління інформаційною

безпекою, або до посадової особи виконкому на яку відповідно до розподілу обов'язків покладені обов'язки системного адміністратора).

4.3. Управління інцидентами інформаційної безпеки

Процедура управління інцидентами інформаційної безпеки скла-дається із декількох етапів.



Основною метою забезпечення інформаційної безпеки (ІБ) виконкому районної в місті ради є зниження ризиків, діючих відносно інформаційних ресурсів, і як наслідок запобігання або мінімізація збитку від можливих інцидентів ІБ.

5. Ролі та відповідальність

Обов'язки щодо своєчасного реагування та розгляду інцидентів інформаційної безпеки покладаються на групу реагування на інциденти інформаційної безпеки (далі - ГРІІБ), яка створюється розпорядженням голови районної в місті ради.

Основні цілі ГРІІБ:

- забезпечення організації кваліфікованим персоналом для обліку, реагування та аналізу інцидентів;
- забезпечення необхідної координації і управління процесом реагування на інциденти;
- забезпечення належного рівня інформування керівництва і зацікавлених осіб;
- забезпечення максимального зниження наслідків інцидентів, як в матеріальній сфері, так і для підтримки репутації організації.

До складу групи рекомендується включити представників наступних структурних підрозділів виконкому районної в місті ради:

- посадову особу виконкому відповідальну за функціонування системи управління інформаційною безпекою (забезпечення координаційної, адміністра-

тивної, експертної і технологічної діяльності);

- працівника, на якого покладено обов'язки служби інформаційних технологій (забезпечення експертної і технологічної діяльності);
- працівника відділу з питань кадрової роботи (забезпечення адміністративної і процедурної діяльності);
- працівника відділу з правових питань (забезпечення експертної і нормативно-правої діяльності);
- працівника відділу, в якому трапився інцидент (залучаються на тимчасовій основі для підтримки забезпечення адміністративної, експертної і технологічної діяльності);
- зовнішніх експертів (забезпечення консультативної, експертної і технологічної діяльності).

6. Документація

Документація повинна містити такі елементи:

- шкалу небезпеки для класифікації інцидентів ІБ (така шкала може складатися, наприклад, з двох положень: "небезпечно" і "безпечно". У будь-якому випадку положення шкали засноване на фактичному або передбачуваному збитку для виконкому районної в місті ради);
- форми звітів про події та інциденти ІБ, відповідні задокументовані методики та дії пов'язані з коректними процедурами використання даних і системи, сервісів і (або) мережевого резервування, планами безперервності управління;
- операційні процедури для ГРІІБ з документованими обов'язками та розподілом функцій серед призначених відповідальних осіб для ведення різних видів діяльності, наприклад таких як:
- відключення ураженої системи, сервісу і (або) мережі, при визначених обставинах за погодженням з відповідним керівництвом і відповідно до попередньої угоди;
- залишення ураженої системи, сервісу і (або) мережі, що знаходиться в працюючому стані;
- ведення моніторингу потоку даних, що виходять, входять або знаходяться в межах ураженої системи, сервісу і (або) мережі;
- активація нормальних дій і процедур планування неперервності управління та резервування згідно політики безпеки системи, сервісу та (або) мережі;
- ведення моніторингу та підтримка безпеки зберігання свідоцтв в електронному вигляді на випадок їх запитання для судового переслідування або внутрішнього дисциплінарного стягнення всередині виконавчого комітету районної в місті ради;
- передача подробиць про інцидент ІБ ГРІІБ, керівництву та стороннім особам або організаціям.

Якщо можливо, документи мають бути в електронній формі (наприклад, на безпечній веб-сторінці) з посиланням на базу даних, що зберігає електронну інформацію про події/інциденти ІБ. Форма заповнюється особою, що робить повідомлення (тобто необов'язково членом ГРІІБ). Форма звіту про інциденти використовується персоналом менеджменту інцидентів ІБ, заповнюється первісною

інформацією про подію ІБ, містить поточні записи оцінки інциденту та інші до повного вирішення інциденту. На кожній стадії в базу даних подій / інцидентів ІБ включаються поновлення. Запис, зроблений у базі даних, що містить "заповнену" форму або відомості про події/інциденти ІБ, потім використовується при розслідуванні інциденту.

7. Коригувальні та превентивні дії

Після усунення наслідків інциденту і відновлення нормального функціонування управлінських процесів виконкому районної в місті ради, виконуються дії щодо запобігання повторного виникнення інциденту. Для визначення необхідності реалізації таких дій проводиться аналіз ризиків, в рамках якого визначається доцільність коригувальних і превентивних дій. В деяких випадках, якщо наслідки інциденту незначні в порівнянні з коригувальними і превентивними діями, тоді доцільно не виконувати подальших кроків після усунення наслідків інциденту.

Керуючий справами виконкому ***Олександр Гижко***

Додаток 1
до Методики виявлення
та реєстрації інцидентів
інформаційної безпеки

Реєстр інцидентів
виконавчого комітету Довгинцівської районної в місті ради

Перелік інцидентів ІБ може включати, але не обмежується, наступне:

- зникнення інтернет-зв'язку;
- порушення строків виконання робіт підрядними організаціями;
- припинення дії електронного ключа;
- пожежа;
- викрадення документів;
- викрадення обладнання;
- втрата ключів від приміщень;
- викрадення ключів від приміщень;
- збої у системі живлення;
- відключення подачі електроенергії;
- спроба ураження;
- ураження вірусами;
- відсутність ліцензій на продукт;
- витік інформації через ПЗ;
- витік інформації через персонал;
- непрацездатність ПЗ електронного документообігу;
- непрацездатність обладнання, систем (апаратної частини);
- пошкодження документів внаслідок невідповідних кліматичних умов (вологості, освітлення);
- викрадення даних із ПК;
- не зроблене резервування даних;
- порушення цілісності ПЗ або ПК;
- несанкціонований доступ до даних,
- несанкціоноване внесення змін до даних;
- збій у системі (-ах) (через неправильне поводження з нею тощо);
- відкриття доступу до секретних даних;
- несанкціоноване обмеження доступу до інформації;
- втрата документів під час переміщення з підрозділу до підрозділу;
- вихід із строю обладнання через природні явища;
- прослуховування телефонних розмов;
- збій у роботі засобів зв'язку;
- неспроможність зберегти дані (через переповнення дискового простору тощо);
- несанкціонований фізичний доступ до інформації;
- перехоплення факсимільних повідомлень.

Додаток 2
до Методики виявлення
та реєстрації інцидентів
інформаційної безпеки

Інструкція
щодо форми звіту про події та інциденти ІБ
та рекомендації по заповненню

Призначенням форм звіту про події та інциденти ІБ - є забезпечення інформації про подію ІБ, а потім, якщо вона визначена як інцидент, то і про інцидент ІБ для певних осіб. Якщо працівник виконкому підозрює, що подія ІБ розвивається або вже відбулася, особливо таке, яке може завдати істотних втрат або шкоди власності або репутації виконкому районної в місті ради, то він повинен негайно заповнити та передати форму звіту про подію ІБ (див. першу частину додатка 1 до інструкції) посадовій особі виконкому відповідальної за функціонування системи управління інформаційною безпекою або безпосередньо-му керівнику.

Представлена інформація використовується для початку відповідного процесу оцінки, яка визначає, чи повинна ця подія бути категорована як інцидент ІБ чи ні, і в разі позитивної відповіді будуть прийняті необхідні коригувальні заходи для запобігання або обмеження втрат або шкоди. Оскільки цей процес за своїм характером є критичним по часу, то необов'язково заповнювати всі поля у формі звіту в даний момент часу. Якщо Ви є членом групи забезпечення експлуатації, переглядаються вже заповнені / частково заповнені форми, то необхідно вирішити, чи треба категорувати дану подію як інцидент ІБ. Якщо треба, то необхідно заповнити форму для інциденту ІБ наскільки можливо докладно направити і передати форму для події / інциденту ІБ ГРІБ. Незалежно від того, чи буде подія ІБ категорована як інцидент чи ні, в будь-якому випадку база даних подій/інцидентів ІБ повинна бути оновлена.

Форма інциденту ІБ повинна далі оновлюватися в міру прогресу в дослідженні, і відповідні оновлення повинні проводитися в базі даних подій / інцидентів ІБ.

При заповненні форм виконуються наступні рекомендації:

- якщо можливо, то форми повинні заповнюватися і передаватися в електронному вигляді[1]. Якщо існують проблеми або вважається, що існують проблеми з встановленими за замовчуванням механізмами електронного оповіщення (наприклад, електронна пошта), включаючи випадки, коли система, можливо, піддається атаці, і форми звіту можуть бути прочитані неавторизованими особами, тоді повинні використовуватися альтернативні засоби зв'язку. Альтернативними засобами зв'язку можуть бути телефон або текстові повідомлення;

---

[1] Якщо можливо, то ці форми повинні бути в електронному вигляді (наприклад, на безпечній web-сторінці) з прив'язкою до електронної бази даних подій / інцидентів ІБ. У сучасному світі, заснована на паперовій документації система є занадто повільною і далеко не найефективнішою в експлуатації.

- уявляйте інформацію, засновану тільки на фактах, в якій Ви впевнені, нічого не придумуйте для того, щоб заповнити всі поля. Де доречно включити інформацію, яку Ви не можете підтвердити, чітко вкажіть, що це непідтверджена інформація і чому Ви вважаєте, що вона вірна;
- Ви повинні докладно вказати, як можна з Вами зв'язатися. Дуже скоро або через деякий час може виникнути необхідність контакту з Вами для подальшої інформації, що стосується Вашого звіту.

Якщо пізніше працівником виконкому буде виявлено, що деяка представлена інформація неточна, неповна або помилкова, то він повинен внести поправки в звіт і надати його повторно.

Звіт про подію ІБ

Дата події
Номер події (назначається керівником ГРІБ):

(Якщо потрібно) відповідні ідентифікаційні номери подій і (або) інцидентів:

Інформація про особу, що повідомляє:
Прізвище
_____
Адреса
_____
Організація
_____
Телефон
_____
Електронна пошта
_____

Опис події ІБ

Опис події:
· Що сталося
_____
· Як сталося
_____
· Чому відбулося
_____
· Уражені компоненти
_____
· Негативний вплив на службову діяльність
_____
· Будь-які ідентифіковані уразливості
_____

Деталі події ІБ
Дата і час виникнення події

_____
Дата і час виявлення події

_____
Дата і час повідомлення про подію

_____
Чи закінчилася подія? (Зазначити квадрат) | так | | ні |

Якщо «так», то уточнити, як довго тривала подія в днях / годинах / хвилинах.

Звіт про інцидент ІБ

Дата інциденту
Номер інциденту (призначаються керівником ГРІБ і прив'язуються до номера (-ам) відповідних подій):

(Якщо потрібно) відповідні ідентифікаційні номери подій і (або) інцидентів:

Інформація про співробітника групи забезпечення експлуатації:
Прізвище _____
Адреса _____
Телефон _____
Електронна пошта _____

Інформація про співробітника ГРІБ:
Прізвище _____
Адреса _____
Телефон _____
Електронна пошта _____

Опис інциденту ІБ
Подальший опис інциденту:
· Що сталося _____
· Як сталося _____
· Чому відбулося _____
· Уражені компоненти _____
· Негативний вплив на службову діяльність _____
· Будь-які ідентифіковані уразливості _____

Деталі інциденту ІБ:
Дата і час виникнення інциденту _____
Дата і час виявлення інциденту _____
Дата і час повідомлення про інцидент _____

Закінчився інцидент? (Зазначити квадрат) | так | ні |
Якщо «так», то уточнити, як довго тривав інцидент в днях / годинах / хвилинах.
Якщо «ні», то уточнити, як довго він уже триває

Тип інциденту ІБ (Відмітити один квадрат, потім заповнити відповідні поля нижче):
Дійсний _____
Спроба _____
Підозра _____

Навмисна (вказати типи загрози) (один з):
Розкрадання (TH) _____
Хакерство / Логічне проникнення (HA) _____
Шахрайство (FR) _____
Неправильне використання ресурсів (MI) _____
Саботаж / фізичний збиток (SA)
Інший збиток (OD)
Шкідлива програма (MC)
Визначити:

Випадкова (вказати типи загрози) (Один з):
Відмова апаратури (HF)
Інші природні події (NE)
Відмова ПО (SF)
Визначити:

Відмова зв'язку (CF)
Втрата істотних сервісів (LE)
Пожежа (HE)
Недостатнє кадрове забезпечення (SS)
Повінь (FL)
Інші випадки (OA)
Визначити:

Помилка (вказати типи загрози) (Один з):
Операційна помилка (OE)
Помилка користувача (UE)
Помилка апаратної підтримки (HE)
Помилка конструкції (DE)
Помилка підтримки ПЗ (SE)
Інші випадки (включаючи справжні омани) (OA)
Визначити:
Невідомо

(Якщо ще не встановлений тип інциденту (навмисний, випадковий, по-милка), то слід зазначити квадрат «невідомо» і, по можливості, вказати тип загрози, використовуючи скорочення, наведені вище)
Визначити:

Уражені активи
Уражені активи (якщо є)
(Дати опису активів, уражених інцидентом, або пов'язаних з ним включаючи серійні, ліцензійні номери та номери версій, по можливості)

Інформація / Дані _____
Апаратура _____
Програмне забезпечення _____
Засоби зв'язку _____
Документація _____
Негативний вплив / вплив інциденту на службову діяльність
Відзначити відповідні квадрати для зазначених нижче порушень, потім в колонці «значимість» вказати рівень негативного впливу за шкалою 1¸ 10, використовуючи скорочення (покажчики категорій): (FD) – фінансові втрати / руйнування бізнес-операцій, (CE) - комерційні і економічні інтереси, (PI) - інформація, що містить персональні дані, (LR) – правові та нормативні зобов'язання (це необхідно звірити з англійським оригіналом), (MO) - менеджмент і службова діяльність, (LG) - втрата престижу. Запишіть кодові букви в колонці «вказівники», а якщо відомі дійсні вартості, то вказати їх у колонці «вартість»

Значимість	Вказівники	Вартість
Порушення конфіденційності (тобто, несанкціоноване розкриття):		
Порушення цілісності (тобто, несанкціонована модифікація):		
Порушення доступності (тобто, недоступність):		
Порушення неспростовності		
Знищення		

Повні вартості відновлення після інциденту

Значимість	Покажчики	Вартість
(Де можливо, необхідно вказати загальні витрати на відновлення після інциденту в цілому по шкалі 1¸ 10 для «значущості» і в грошах для «вартості»)		

Вирішення інциденту

Дата початку розслідування інциденту
_____
Прізвище особи (осіб), що проводив (їх) розслідування інциденту
_____
Дата закінчення інциденту _____
Дата закінчення дії
_____
Дата завершення розслідування інциденту
_____
Посилання та місце зберігання звіту про розслідування
_____

Причетні особи (один з)

Особа (PE)
Легально заснована організація / установа (OI)
Організована група (GR)
Випадковість (AC)
Немає винного (NP)
Наприклад, природні фактори,
Відмова обладнання, помилка людини

Опис порушника
Дійсна або передбачувана мотивація (один з)

Кримінальна / фінансова вигода (CG)
Розвага / хакерство (PH)
Політика / тероризм (PT)
Реванш (RE)
Інші мотиви (OM)
Визначити:

Дії, вжиті для вирішення інциденту
(Наприклад, «ніяких дій», «підручними засобами», «внутрішнє розслідування», «зовнішнє розслідування із залученням ...»)

Дії, заплановані для дозволу інциденту
(Наприклад, див. вище)

Інші дії
(Наприклад, як і раніше потрібне проведення розслідування для іншого персоналу)

Висновок

(Відзначити один з квадратів, чи є інцидент значним чи ні і додати в короткий пояснення для обґрунтування цього висновку)
Значний
Незначний
(Вкажіть будь-які інші висновки) _____

Ознайомлені особи / суб'єкти

(Ця частина звіту заповнюється відповідною особою, на яку покладено обов'язки в області ІБ і яка формулює необхідні дії. Зазвичай цією особою є посадова особа виконкому відповідальна за функціонування системи керування інформаційною безпекою (керівник ІБ).

Керівник ІБ
Керівник ГРІІБ
Місцевий керівник (уточнити, якого підрозділу)
Керівник інформаційних систем
Автор звіту
Керівник автора звіту
Представник РВ МВС(при необхідності)
Інша особа

Визначити:

Залучені особи

Ініціатор
Підпис _____
Прізвище _____
Посада _____
Дата _____

Аналітик
Підпис _____
Прізвище _____
Посада _____
Дата _____

Додаток 5
до розпорядження голови
районної в місті ради
від 24.11.2021 № 345-р

Положення
про застосування цілей заходів інформаційної безпеки у виконкомі Довгинцівської районної в місті ради

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
А.5.Політика безпеки	Забезпечення регулювання та підтримки керівництвом виконкому районної в місті ради інформаційної безпеки згідно з вимогами чинного законодавства України	Так	Закони України:«Про захист персональних даних», «Про інформацію», «Про доступ до публічної інформації»; п.4.2.1.1 Настанови з інформаційної безпеки виконкому Довгинцівської районної в місті ради; додатки 6, 7 цього розпорядження (Політика у сфері інформаційної безпеки та Процедура управління інформаційними активами виконкому Довгинцівської районної в місті ради»))	
А.5.1. Політика інформаційної безпеки				
А.5.1.1. Документ що визначає політику інформаційної безпеки				
А.5.1.2. Аналізування політики інформаційної безпеки		Так	п.4.2.1. Настанови з інформаційної безпеки виконкому Довгинцівської районної в місті ради	
А.6. Організація інформаційної безпеки	Здійснення керування інформаційною безпекою у виконкомі районної в місті ради	Так	п.п 4.1, 5.1 Настанови з інформаційної безпеки виконкому Довгинцівської районної в місті ради	
А.6.1. Внутрішня організація				
А.6.1.1. Зобов'язання керівництва щодо інформаційної безпеки				
А.6.1.2. Координація питань забезпечення інформаційної безпеки		Так	Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради, розпорядження голови районної в місті ради від 24.10.2014 № 205-р «Про розробку системи управління	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	*Цілі заходів безпеки*	*Позначка щодо застосовності (Так, ні, частково)*	*Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки*	*Коментарі (обґрунтування вилучення тощо)*
			інформаційною безпекою у виконкомі районної в місті ради» зі змінами	
А.6.1.3. Розподіл відповідальності щодо забезпечення інформаційної безпеки		Так	п.5.1 Настанови з інформаційної безпеки виконкому Довгинцівської районної в місті ради, додатки 6, 7 цього розпорядження (Політика у сфері інформаційної безпеки та Процедура управління інформаційними активами виконкому Довгинцівської районної в місті ради»)	
А.6.1.4. Процедура отримання дозволу на використання засобів оброблення інформації		Так	Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради	
А.6.1.5. Угоди про дотримання конфіденційності		Так	Закони України: «Про захист персональних даних», «Про інформацію»,«Про доступ до публічної інформації»; «Про службу в органах місцевого самоврядування»	
А.6.1.6. Взаємодія з компетентними органами		Так	Закон України «Про службу в органах місцевого самоврядування»	
А.6.1.7. Взаємодія з професійними групами		Так	Договори щодо технічного обслуговування комп'ютерної та оргтехніки, вебсайту виконкому районної в місті ради	
А.6.1.8. Незалежна перевірка (аудит) безпеки інформації		Так	п.п. 4.2.4, 7 Настанови з інформаційної безпеки виконкому Довгинцівської районної в місті ради	
А.6.2. Зовнішні сторони А.6.2.1. Визначення ризиків, що зі сторонніми організаціями	Підтримка в актуальному стані безпеки інформації виконкому районної в місті ради та засобів оброблення інформації, до яких мають доступ, обробляють, якими управляють	Так	п.4.2.1.2 Настанови з інформаційної безпеки виконкому Довгинцівської районної в місті ради; «Методика управління ризиками у виконкомі Довгинцівської районної в місті ради» (додаток 10 цього розпорядження)	
А.6.2.2. Розгляд питань безпеки щодо роботи з клієнтами		Так	Закони України: «Про захист персональних даних», «Про інформацію»,«Про доступ до публічної інформації»; Регламент виконкому;	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
	або з якими підтримують зв'язок зовнішні сторони		Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради	
А.6.2.3. Розгляд вимог щодо безпеки в угодах зі сторонніми організаціями		Так	Розпорядження голови районної в місті ради «Про заходи щодо виконання Закону України «Про захист персональних даних», договори щодо технічного обслуговування комп'ютерної та оргтехніки, вебсайту виконкому районної в місті ради	
А.7. Управління активами	Досягнення та підтримка належного захисту ресурсів системи керування інформаційною безпекою виконкому районної в місті ради	Так	п. 5.2 Настанови з інформаційної безпеки виконкому Довгинцівської районної в місті ради; посадові інструкції посадових осіб структурних підрозділів виконкому; Реєстр інформаційних активів виконкому Довгинцівської районної в місті ради (додаток 8 цього розпорядження)	
А.7.1.Відповідальність за захист активів організації				
А.7.1.1. Інвентаризація активів		Так	п. 5.2.1 Настанови з інформаційної безпеки виконкому Довгинцівської районної в місті ради; Реєстр інформаційних активів виконкому Довгинцівської районної в місті ради (додаток 8 цього розпорядження)	
А.7.1.2. Володіння активами		Так	п. 5.2.1 Настанови з інформаційної безпеки виконкому Довгинцівської районної в місті ради; Реєстр інформаційних активів виконкому Довгинцівської районної в місті ради (додаток 8 цього розпорядження)	
А.7.1.3. Прийнятне використання активів		Так	п. 5.2 Настанови з інформаційної безпеки виконкому Довгинцівської районної в місті ради; договори щодо технічного обслуговування комп'ютерної та оргтехніки, вебсайту виконкому районної в місті ради	
А.7.2. Класифікація інформації	Забезпечення належного рівня захисту інформації	Так	Закон України «Про інформацію»; Закон України «Про доступ до публічної інформації»; Закон України «Про державну таємницю»; Закон України «Про захист	
А.7.2.1 Основні принципи класифікації				

Розділи додатку А ДСТУ ISO/IEC 27001:2015	*Цілі заходів безпеки*	*Позначка щодо застосовності (Так, ні, частково)*	*Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки*	*Коментарі (обґрунтування вилучення тощо)*
			персональних даних»; Наказ СБУ від 23.12.2020 № 383 «Про затвердження Зводу відомостей, що становлять державну таємницю» зі змінами; Постанова КМУ від 19 жовтня 2016 р. № 736 «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію»; 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	
А.7.2.2. Маркування та оброблення інформації		Так	Постанови Кабінету Міністрів України від 27 квітня 1993 року № 301 «Про трудові книжки працівників»; -рішення виконкому Криворізької міської ради від 12.09.2018 № 428 «Про затвердження Інструкції з діловодства в органах місцевого самоврядування міста» зі змінами, рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами	
А.8. Правила безпеки, пов’язані з персоналом	Забезпечення гарантії, що найманий персонал, підрядники та користувачі третьої сторони розуміють свої обов'язки, придатні до ролей, на які претендують; зменшення ризику	Так	Закон України «Про службу в органах місцевого самоврядування»; рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами	
А.8.1. До праце-влаштування				
А.8.1.1. Ролі та відповідальність персоналу щодо забезпечення безпеки		Так	Закон України «Про службу в органах місцевого самоврядування»; рішення виконкому районної в місті ради від 17.04.2019 № 143	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	*Цілі заходів безпеки*	*Позначка щодо застосовності (Так, ні, частково)*	*Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки*	*Коментарі (обґрунтування вилучення тощо)*
	розкрадання, шахрайства чи зловживання обладнанням		«Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Положення про відділ, посадові інструкції працівників виконкому районної в місті ради	
А.8.1.2. Перевіряння під час приймання на роботу		Так	Розпорядження голови районної в місті ради «Про затвердження Порядку організації проведення спеціальної перевірки відомостей щодо осіб, які претендують на зайняття посад посадових осіб місцевого самоврядування у виконкомі районної в місті ради»	
А.8.1.3. Умови трудового договору		Так	Закон України «Про службу в органах місцевого самоврядування», Постанова Кабінету Міністрів України від 15 лютого 2002 року №169 «Про затвердження Порядку проведення конкурсу на заміщення вакантних посад державних службовців» зі змінами	
А.8.2. Під час виконання своїх службових обов’язків	Забезпечення: поінформова-ності найманого персоналу, підрядників та користувачів третьої сторони стосовно загроз і проблем інформаційної безпеки, відповідальності та обов'язків у сфері інформаційної безпеки;	Так	Закон України «Про службу в органах місцевого самоврядування»; рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Наказ Національного агентства України з питань державної служби від 05.08.2016 № 158 «Про затвердження Загальних правил етичної поведінки державних службовців та посадових осіб місцевого самоврядування» зі змінами.	
А.8.2.1. Зобов’язання керівництва	працівників усім необхідним для підтримки політики безпеки виконкому районної в місті ради в ході повсякденної	Так	п. 5.1 Настанови з інформаційної безпеки виконкому Довгинцівської районної в місті ради; додатки 6, 7 цього розпорядження (Політика у сфері інформаційної безпеки та Процедура управління інформаційними активами виконкому Довгинцівської	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	*Цілі заходів безпеки*	*Позначка щодо застосовності (Так, ні, частково)*	*Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки*	*Коментарі (обґрунтування вилучення тощо)*
	роботи та зменшення ризику суб'єктивної помилки		районної в місті ради»).	
А.8.2.2. Обізнаність, навчання, перепідготовка у сфері інформаційної безпеки		Так	п. 5.2.2 Настанови з інформаційної безпеки виконкому Довгинцівської районної в місті ради; Закон України «Про службу в органах місцевого самоврядування»; Постанова КМУ від 6 лютого 2019р. № 106 «Про затвердження Положення про систему професійного навчання державних службовців, голів місцевих державних адміністрацій, їх перших заступників та заступників, посадових осіб місцевого самоврядування та депутатів місцевих рад»	
А.8.2.3. Дисциплінарна практика		Так	Закони України «Про захист персональних даних», «Про службу в органах місцевого самоврядування», Кодекс законів про працю	
А.8.3. Звільнення або змінення службових обов’язків	Забезпечення гарантій, що весь найманий персонал, підрядники та користувачі третьої сторони залишають виконком районної в місті ради чи змінюють умови найму в установленому порядку	Так	Закони України «Про захист персональних даних», «Про службу в органах місцевого самоврядування», Кодекс законів про працю	
А.8.3.1. Відповідальність після закінчення дії трудового договору		Так	Закони України «Про захист персональних даних», «Про службу в органах місцевого самоврядування», Кодекс законів про працю	
А.8.3.2. Повернення активів		Так	Закони України «Про захист персональних даних», «Про службу в органах місцевого самоврядування»; Кодекс законів про працю	
А.8.3.3. Анулювання прав доступу		Так	Закони України «Про захист персональних даних», «Про службу в органах місцевого самоврядування» Кодекс законів про працю	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
А.9. Фізична та екологічна безпека А.9.1. Безпечні зони	Запобігання несанкціонованому у фізичному доступу, ушкодженню та вторгненню до службових приміщень виконкому районної в місті ради та втручанню в його інформацію	Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. «Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради» (додаток 12 цього розпорядження)	
А.9.1.1. Периметр зон, які охороняють		Так	«Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради» (додаток 12 цього розпорядження)	
А.9.1.2. Контролювання доступу в зону, яку охороняють		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. «Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради» (додаток 12 цього розпорядження)	
А.9.1.3. Забезпечення безпеки будівель, виробничих приміщень та устаткування		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. «Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради» (додаток 12 цього розпорядження)	
А.9.1.4. Захист від зовнішніх впливів та загроз з боку довкілля		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. «Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради» (додаток 12 цього розпорядження)	
А.9.1.5. Робота в зонах, які		Так	Угоди про співробітництво щодо технічного обслуговування	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
охороняють			комп'ютерної та оргтехніки, іншого обладнання «Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради» (додаток 12 цього розпорядження)	
А.9.1.6. Зони громадського доступу, прийому та відвантаження матеріальних цінностей		Так	«Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради» (додаток 12 цього розпорядження)	
А.9.2. Забезпечення безпеки устаткування	Запобігання втратам, ушкодженню, крадіжці або компрометації ресурсів системи керування інформаційною безпекою та перериванню діяльності виконкому районної в місті ради	Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. «Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради» (додаток 12 цього розпорядження)	
А.9.2.1. Розміщення та захист устаткування		Так	«Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради» (додаток 12 цього розпорядження)	
А.9.2.2. Допоміжні послуги		Так	«Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради» (додаток 12 цього розпорядження)	
А.9.2.3. Безпека кабельної мережі		Так	«Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради» (додаток 12 цього розпорядження)	
А.9.2.4. технічне обслуговування устаткування		Так	«Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради» (додаток 12 цього розпорядження) Угоди про співробітництво щодо технічного обслуговування комп'ютерної та оргтехніки, іншого обладнання	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	*Цілі заходів безпеки*	*Позначка щодо застосовності (Так, ні, частково)*	*Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки*	*Коментарі (обґрунтування вилучення тощо)*
А.9.2.5. Забезпечення безпеки устаткування, яке використовують за межами приміщень організації		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. «Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради» (додаток 12 цього розпорядження)	
А.9.2.6. Безпечна утилізація або повторного використання устаткування		Так	«Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради» » (додаток 12 цього розпорядження)	
А.9.2.7. Перенесення майна за межі організації		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. «Положення про фізичну та екологічну безпеку інформації виконкому Довгинцівської районної в місті ради» (додаток 12 цього розпорядження)	
А. 10. Управління засобами комунікації та їх функціюванням А. 10.1. Процедури щодо експлуатації. Відповідальність	Забезпечення коректного та безпечного функціонування засобів оброблення інформації	Так	Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради; Регламент виконкому	
А. 10.1.1. Документування експлуатаційних процедур		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
А. 10.1.2. Управління змінами		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами	
А. 10.1.3. Розмежування обов'язків		Так	Закон України «Про службу в органах місцевого самоврядування»; Посадові інструкції; Положення про структурні підрозділи;	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
			Регламент виконкому	
А. 10.1.4. Розмежування засобів розроблення, тестування та експлуатації		Так	Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради	
А.10.2. Управління наданням послуг сторонніми організаціями	Впровадження та підтримка належного рівня інформаційної безпеки й надання послуг відповідно до угод щодо надання послуг третьою стороною	Так	Угоди про співробітництво щодо технічного обслуговування комп'ютерної та оргтехніки	
А. 10.2.1. Надання послуг		Так	Угоди про співробітництво щодо технічного обслуговування комп'ютерної та оргтехніки	
А. 10.2.2. Моніторинг та аналізування послуг, наданих сторонніми особами та/чи організаціями		Так	Угоди про співробітництво щодо технічного обслуговування комп'ютерної та оргтехніки	
А. 10.2.3. Зміни у разі надання сторонніми організаціями послуг щодо забезпечення безпеки		Так	Угоди про співробітництво щодо технічного обслуговування комп'ютерної та оргтехніки	
А. 10.3. Планування та приймання систем	Мінімізування ризику відмови систем	Так	Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради; Угоди про співробітництво щодо технічного обслуговування комп'ютерної та оргтехніки	
А.10.3.1. Управління продуктивністю		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами	
А.10.3.2. Приймання систем		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Угоди про співробітництво щодо технічного обслуговування комп'ютерної та оргтехніки	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
А. 10.4. Захист від шкідливого та мобільного коду	Захист цілісності програмного забезпечення та інформації	Так	4.2.2 Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради; План зниження ризиків у виконкомі Довгинцівської районної в місті ради	
А. 10.4.1. Заходи захисту від шкідливого коду		Так	4.2.2 Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради; План зниження ризиків у виконкомі Довгинцівської районної в місті ради	
А. 10.4.2. Заходи захисту від мобільного коду		Так	4.2.2 Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради; План зниження ризиків у виконкомі Довгинцівської районної в місті ради	
А. 10.5 Резервування	Підтримування цілісності і доступності інформації та засобів оброблення інформації	Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Експлуатаційна документація	
А. 10.5.1 Резервування інформації				
А. 10.6 Управління безпекою мереж	Забезпечення захисту інформації в мережах і захисту інфраструктури, що їх підтримує	Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
А. 10.6.1 Засоби контролювання мереж		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
А. 10.6.2 Безпека мережевих сервісів		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами	
А. 10.7 Поводження з носіями інформації	Запобігання несанкціонованому розголошенню, модифікації, вилученню або знищенню активів, а також	Так	Розпорядження голови районної у місті ради «Про заходи щодо виконання Закону України «Про захист персональних даних»	
А. 10.7.1 Управління знімними носіями		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження)	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
інформації	перерванню діяльності			
А.10.7.2 Утилізація носіїв інформації		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження)	
А. 10.7.3. Процедура оброблення інформації		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
А. 10.7.4. Безпека системної документації		Так	Посадові інструкції; Експлуатаційна документація; Постанови Кабінету Міністрів України від 27 квітня 1993 року № 301 «Про трудові книжки працівників» зі змінами	
А.10.8 Обмін інформацією	Підтримка безпеки інформації і програмного забезпечення в разі обміну всередині виконкому та зі сторонніми організаціями	Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
А. 10.8.1 Політика та процедури обміну інформацією		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
А.10.8.2 Угода щодо обміну інформацією		Так	Угоди/договори про співпрацю із підрядниками та постачальниками	
А.10.8.3. Захист фізичних носіїв під час транспортування		Так	Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради; Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження)	
А. 10.8.4 Електронний обмін повідомленнями		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Угоди/договори про співпрацю із підрядниками та постачальниками	
А.10.8.5 Інформаційні системи		Так	Експлуатаційна документація	
А. 10.9 Послуги електронної комерції	Забезпечення безпеки послуг електронної	Ні	-	Фізич-но не існують

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
А. 10.9.1 Електронна комерція	комерції та їх безпечне використання	Ні	-	Фізич-но не існує
А. 10.9.2 Трансакції в режимі реального часу (онлайн)		Ні	-	Фізич-но не існує
А. 10.9.3 Загальнодоступна інформація		Так		
А. 10.10 Моніторинг	Виявлення несанкціонова-них дій щодо оброблення інформації	Так	Посадові інструкції	
А.10.10.1 Ведення журналів аудиту		Так	Посадові інструкції; Експлуатаційна документація	
А.10.10.2 Моніторинг використання засобів оброблення інформації		Так	Посадові інструкції; Експлуатаційна документація	
А.10.10.3. Захист інформації журналів реєстрації		Так	Посадові інструкції; Експлуатаційна документація; рішення виконкому міської ради від 12.09.2018 № 428 «Про затвердження Інструкції з діловодства в органах місцевого самоврядування міста» зі змінами	
А. 10.10.4. Журнали реєстрації дій адміністратора та оператора		Так	Посадові інструкції; Експлуатаційна документація;	
А.10.10.5 Реєстрація відмов		Так	Службові записки стосовно обслуговування комп'ютерної та оргтехніки	
А.10.10.6. Синхронізація годинників		Так	Експлуатаційна документація	
А.11 Управління доступом				
А.11.1. Вимоги до управління доступом	Контроль доступу до інформації	Так	Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради; Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
			місті ради» зі змінами.	
A.11.1.1. Політика контролювання доступу		Так	Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради; Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
A.11.2. Управління доступом користувачів	Запобігання несанкціонованому доступу користувачів до інформаційних систем та забезпечення авторизованого доступу користувачів до цих систем	Так	Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради; Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
A.11.2.1. Реєстрація користувачів		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
A.11.2.2. Управління привілеями		Так	Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради; Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
A.11.2.3. Управління паролями користувачів		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
A.11.2.4 Перегляд прав доступу користувачів		Так	Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради; Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
A.11.3 Відповідальність користувачів	Запобігання несанкціонованому доступу користувачів, а також компрометації або крадіжці інформації та засобів оброблення інформації	Так	Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради; Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
A.11.3.1 Використання паролів		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
A.11.3.2 Устаткування, яке залишене користувачем без нагляду		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
А.11.3.3 Правила «чистого стола» та «чистого екрану»		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
А.11.4 Управління доступом до мережі	Запобігання несанкціонованому доступу до мережевих послуг	Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Експлуатаційна документація	
А.11.4.1 Політика щодо використання мережевих послуг		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
А.11.4.2 Аутентифікація користувачів щодо зовнішніх з'єднань		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Експлуатаційна документація	
А.11.4.3 Ідентифікація устаткування в мережах		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Експлуатаційна документація	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
А.11.4.4 Захист діагностичних і конфігураційних портів під час віддаленого доступу		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Експлуатаційна документація	
А. 11.4.5 Принцип розподілу в мережі		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Експлуатаційна документація	
А. 11.4.6 Контролювання мережевих з'єднань		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Експлуатаційна документація	
А. 11.4.7 Контролювання маршрутизації в мережі		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Експлуатаційна документація	
А.11.5 Контролювання доступу до операційної системи	Запобігання несанкціонованому доступу до операційних систем	Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Експлуатаційна документація	
А. 11.5.1 Безпечні процедури		Так	Політики і принципи інформаційної безпеки (додаток 2	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	*Цілі заходів безпеки*	*Позначка щодо застосовності (Так, ні, частково)*	*Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки*	*Коментарі (обґрунтування вилучення тощо)*
реєстрації			цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Експлуатаційна документація	
A.11.5.2 Ідентифікація та аутентифікація користувача		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
A.11.5.3 Система управління паролями		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
A.11.5.4 Використання системних утиліт		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Експлуатаційна документація	
A.11.5.5 Період бездіяльності в сеансі зв’язку		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
A.11.5.6. Обмеження часу з’єднання		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
			місті ради» зі змінами. Експлуатаційна документація.	
А.11.6. Управління доступом до прикладних програм та інформації	Запобігання несанкціонованому доступу до прикладних систем та інформації	Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Закони України: «Про захист персональних даних», «Про інформацію», «Про доступ до публічної інформації»	
А.11.6.1 Обмеження доступу до інформації		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Закони України: «Про захист персональних даних», «Про інформацію», «Про доступ до публічної інформації»	
А.11.6.2 Ізоляція систем, що оброблюють важливу інформацію		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
А.11.7 Мобільні обчислення	Забезпечення інформаційної безпеки під час використання переносних пристроїв та засобів, необхідних для роботи в дистанційному режимі	Ні	-	Фізично не існує
А.11.7.1 Робота з переносними пристроями		Так	Політики і принципи інформаційної безпеки (додаток 2 цього розпорядження); Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
А.11.7.2 Робота в дистанційному		Ні	-	Не викону-

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
режимі				ється
А. 12 Розроблення, впровадження та обслуговування інформаційних систем	Забезпечення безпеки як невід'ємної частини інформаційних систем	Так	«Положення про придбання, розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження); Ліцензійні угоди	
А. 12.1 Вимоги щодо безпеки інформаційних систем				
А.12.1.1 Аналіз й деталізація вимог щодо безпеки		Так	«Положення про придбання, розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження); Ліцензійні угоди	
А. 12.2 Правильне оброблення даних у застосуваннях	Запобігання помилкам, втратам, несанкціонованій модифікації або неправильному використанню інформації в застосуваннях	Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. «Положення про придбання, розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження)	
А. 12.2.1 Перевіряння достовірності вхідних даних		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. «Положення про придбання, розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження)	
А. 12.2.2 Контролювання оброблення даних у застосуваннях		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. «Положення про придбання, розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження)	
А. 12.2.3 Цілісність повідомлення		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
			«Положення про придбання, розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження)	
А. 12.2.4 Підтвердження достовірності вихідних даних		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. «Положення про придбання, розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження)	
А.12.3 Криптографічне контролювання	Забезпечення захисту конфіденційності, аутентичності або цілісності інформації криптографічними засобами	Так	Експлуатаційна документація комплексної системи захисту інформації (АІТС «Державний реєстр виборців», ЄІАС «Діти»); Накази та робочі інструкції відділу ведення Державного реєстру виборців та служби у справах дітей	
А.12.3.1. Політика використання криптографічного контролю		Так	Експлуатаційна документація комплексної системи захисту інформації (АІТС «Державний реєстр виборців», ЄІАС «Діти»); Накази та робочі інструкції відділу ведення Державного реєстру виборців та служби у справах дітей	
А.12.3.2. Управління ключами		Так	Експлуатаційна документація комплексної системи захисту інформації (АІТС «Державний реєстр виборців», ЄІАС «Діти»); Накази та робочі інструкції відділу ведення Державного реєстру виборців та служби у справах дітей	
А. 12.4. Безпека системних файлів	Забезпечення безпеки системних файлів	Так	«Положення про придбання, розробку та обслуговування інформаційних систем» » (додаток 11 цього розпорядження); Посадові інструкції	
А. 12.4.1 Контролювання програмного забезпечення, що перебуває в		Так	«Положення про придбання, розробку та обслуговування інформаційних систем» » (додаток 11 цього розпорядження); Посадові інструкції	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
експлуатації				
А. 12.4.2 Захист даних тестування системи		Так	«Положення про придбання, розробку та обслуговування інформаційних систем» » (додаток 11 цього розпорядження)	
А. 12.4.3 Контролювання доступу до початкових кодів		Так	«Положення про придбання, розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження)	
А 12.5 Безпека в процесах розроблення та підтримування	Підтримування безпеки програмного забезпечення прикладних систем та їхньої інформації	Так	«Положення про придбання, розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження); Ліцензійні угоди	
А. 12.5.1 Процедури контролю змінами		Так	«Положення про придбання, розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження); Ліцензійні угоди	
А. 12.5.2 Технічний огляд прикладних систем після внесення змін в операційні системи		Так	«Положення про придбання, розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження); Ліцензійні угоди	
А.12.5.3 Обмеження на внесення зміни у пакети програм		Так	«Положення про придбання, розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження); Ліцензійні угоди	
А.12.5.4 Витік інформації		Так	«Положення про придбання, розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження); Ліцензійні угоди	
А.12.5.5 Розроблення програмного забезпечення із залученням сторонніх організацій		Так	«Положення про придбання, розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження); Ліцензійні угоди	
А.12.6 Управління технічними уразливостями	Зниження ризиків, які є результатом використання відомих технічних уразливостей	Так	«Положення про придбання, розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження); Ліцензійні угоди	
А. 12.6.1		Так	«Положення про придбання,	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
Контролювання за технічними уразливостями			розробку та обслуговування інформаційних систем» (додаток 11 цього розпорядження); Ліцензійні угоди	
А.13 Управління інцидентом інформаційної безпеки	Забезпечення оперативності повідомлення стосовно події щодо інформаційної безпеки та порушень, пов'язаних інформаційними системами, а також своєчасності коригувальних дій	Так	«Методика виявлення та реєстрації інцидентів у виконкомі Довгинцівської районної в місті ради» (додаток 4 цього розпорядження)	
А.13.1 Повідомлення про порушення та недоліки інформаційної безпеки		Так	«Методика виявлення та реєстрації інцидентів у виконкомі Довгинцівської районної в місті ради» (додаток 4 цього розпорядження)	
А. 13.1.1 Повідомлення щодо випадків порушення інформаційної безпеки		Так	«Методика виявлення та реєстрації інцидентів у виконкомі Довгинцівської районної в місті ради» (додаток 4 цього розпорядження)	
А.13.1.2. Повідомлення про недоліки безпеки		Так	«Методика виявлення та реєстрації інцидентів у виконкомі Довгинцівської районної в місті ради» (додаток 4 цього розпорядження)	
А. 13.2 Управління інцидентами інформаційної безпеки та його вдосконаленням	Забезпечення послідовного та ефективного підходу до управління ін-цидентами інформаційної безпеки	Так	«Методика виявлення та реєстрації інцидентів у виконкомі Довгинцівської районної в місті ради» (додаток 4 цього розпорядження)	-
А.13.2.1. Відповідальності та процедури		Так	«Методика виявлення та реєстрації інцидентів у виконкомі Довгинцівської районної в місті ради» (додаток 4 цього розпорядження)	
А.13.2.2. Отримання досвіду на основі інцидентів інформаційної безпеки		Так	«Методика виявлення та реєстрації інцидентів у виконкомі Довгинцівської районної в місті ради» (додаток 4 цього розпорядження)	
А. 13.2.3. Збір доказів		Так	«Методика виявлення та реєстрації інцидентів у виконкомі Довгинцівської районної в місті ради» (додаток 4 цього розпорядження)	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
А. 14. Управління безперервністю діяльності				
А. 14.1. Аспекти інформаційної безпеки управління безперервністю діяльності	Протидія перериванням у діяльності та захист критичних процесів від впливу серйозних відмов інформаційних систем чи лиха й забезпечення їх своєчасного відновлення	Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
А. 14.1.1. Включення інформаційної безпеки в процесі управління безперервністю діяльності		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами.	
А. 14.1.2. Безперервність діяльності й оцінка ризику		Так	«Методика управління ризиками у виконкомі Довгинцівської районної в місті ради (додаток 10 цього розпорядження)	
А. 14.1.3. Розроблення та впровадження планів безперервності діяльності, що містять інформаційну безпеку		Так	«Методика управління ризиками у виконкомі Довгинцівської районної в місті ради (додаток 10 цього розпорядження)	
А. 14.1.4. Структура плану забезпечення безперервності діяльності		Так	«Методика управління ризиками у виконкомі Довгинцівської районної в місті ради (додаток 10 цього розпорядження)	
А. 14.1.5. Тестування, підтримка та перегляд планів щодо безперервності діяльності		Так	«Методика управління ризиками у виконкомі Довгинцівської районної в місті ради (додаток 10 цього розпорядження)	
А. 15. Відповідність				
А. 15.1. Відповідність правовим вимогам	Запобігання будь-яким порушенням норм кримінального та цивільного права,	Так	Закони України "Про місцеве самоврядування в Україні", "Про захист персональних даних", "Про доступ до публічної інформації", "Про інформацію"	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
А. 15.1.1. Визначення норм, які застосовують	вимог, встановлених нормативно-правовими актами, регулювальними органами або договірними зобов'язаннями, а також вимог щодо безпеки	Так	Закони України "Про місцеве самоврядування в Україні", "Про захист персональних даних", "Про доступ до публічної інформації", "Про інформацію"; Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради	
А.15.1.2. Права на інтелектуальну власність		Так	Ліцензійні угоди	
А. 15.1.3. Захист записів організації		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради	
А. 15.1.4. Захист даних і конфіден-ційність персо-нальних даних		Так	Закон України «Про захист персональних даних», Розпорядження голови районної у місті ради"Про заходи щодо виконання Закону України "Про захист персональних даних"	
А.15.1.5 Запобігання нецільовому використанню засобів оброблення інформації		Так	Рішення виконкому районної в місті ради від 17.04.2019 № 143 «Про затвердження Регламенту виконавчого комітету районної в місті ради» зі змінами. Посадові інструкції	
А.15.1.6 Регулювання використання криптографічного захисту		Так	Експлуатаційна документація комплексної системи захисту інформації (АІТС «Державний реєстр виборців», ЄІАС «Діти»); Накази та робочі інструкції відділу ведення Державного реєстру виборців та служби у справах дітей	
А.15.2. Відповідність політикам і стандартам щодо безпеки та технічна відповідність вимогам щодо безпеки	Забезпечення відповідності систем організаційним політикам і стандартам щодо безпеки	Так	Закони України:«Про захист персональних даних», «Про інформацію», «Про доступ до публічної інформації»; Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради	

Розділи додатку А ДСТУ ISO/IEC 27001:2015	***Цілі заходів безпеки***	***Позначка щодо застосовності (Так, ні, частково)***	***Документи (політики, правила, інструкції тощо), які регламентують використання заходів безпеки***	***Коментарі (обґрунтування вилучення тощо)***
А.15.2.1 Відповідність політикам та стандартам безпеки		Так	Закони України:«Про захист персональних даних», «Про інформацію», «Про доступ до публічної інформації»; Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради	
А.15.2.2 Перевіряння технічної відповідності вимогам щодо безпеки		Так	Експлуатаційна документація	
А.15.3. Розгляди аудиту інформаційних систем	Підвищення ефективності процесу аудиту інформаційних систем та зниження негативного впливу на цей процес	Так	Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради	
А.15.3.1. Заходи управління аудитом інформаційних систем		Так	Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради	
А.15.3.2 Захист інструментальних засобів аудиту інформаційних систем		Так	Настанова з інформаційної безпеки виконкому Довгинцівської районної в місті ради	

Керуючий справами виконкому ***Олександр Гижко***

Додаток 6
до розпорядження голови
районної в місті ради
від 24.11.2021 № 345-р

Політика
у сфері інформаційної безпеки
виконкому Довгинцівської районної в місті ради

I. Місія

1.1. Створення відкритих, зручних і доступних умов для отримання якісних послуг мешканцями району.

1.2. Розвиток інформаційної інфраструктури виконкому районної в місті ради, забезпечення її відкритості, мобільності, удосконалення і автоматизації процесів у роботі з інформацією, впровадження новітніх інформаційно-комунікаційних технологій та захисту інформації.

1.3. Впровадження ефективної системи управління інформаційною безпекою, гарантування безпечності та надійності функціонування всіх процесів виконкому районної в місті ради, виконання вимог чинного законодавства України в частині захисту персональних даних, збереження найбільш цінної для виконкому та громадян інформації.

II. Пріоритети діяльності

2.1. Реалізація державної політики щодо захисту інтересів суспільства та територіальної громади.

2.2. Досягнення високого рівня якості надання публічних, у т.ч. адміністративних послуг через використання сучасних безпечних інформаційних технологій.

2.3. Забезпечення оперативної та надійної взаємодії всіх рівнів управління у вирішенні завдань розвитку району, надання широкого спектра інформаційних послуг його мешканцям.

2.4. Забезпечення безпеки інформаційних ресурсів виконкому з урахуванням кращих практик та відповідно до вимог чинного законодавства України.

2.5. Зменшення рівня ризиків у сфері інформаційної безпеки.

2.6. Захист інформаційних активів.

2.7. Підвищення продуктивності роботи працівників і ефективності прийняття рішень.

III. Принципи діяльності

3.1. Відкритість, достовірність та доступність для громадян інформації про діяльність, рішення та можливості органів місцевого самоврядування.

3.2. Інтегрованість – забезпечення зберігання й обробки інформації у виконкомі районної в місті ради в єдиному інформаційному просторі.

3.3. Адаптованість забезпечення високого ступеня захисту інформації від несанкціонованого доступу та руйнування.

3.4. Розширюваність – нарощування функціональних можливостей інформаційної інфраструктури виконкому районної в місті ради, її модифікація.

3.5. Якість – повнота, узгоджуваність усіх даних інформаційного середовища, розмежування повноважень та прав доступу до інформаційних ресурсів.

3.6. Узгодженість пріоритетів інформаційної безпеки з основними напрямами Програми соціально-економічного та культурного розвитку району.

3.7. Збереження прав громадян на захист персональних даних.

3.8. Системний та процесний підхід до діяльності й забезпечення інформаційної безпеки.

3.9. Застосування кращих практик управління інформаційною безпекою.

3.10. Збереження балансу між конфіденційністю, цілісністю та доступністю інформації.

IV. Реалізація пріоритетів

Реалізація пріоритетів досягається через:

4.1 регулювання відносин, пов’язаних із захистом інформації відповідно до наданих повноважень, порядку доступу до інформаційних активів у межах існуючого права на їх використання, відповідальність за порушення встановлених вимог;

4.2 упровадження заходів, що забезпечують захист інформаційних активів;

4.3 ведення обліку законодавчих та нормативних вимог в сфері інформаційної безпеки;

4.4 забезпечення:

4.4.1 відповідної кваліфікації персоналу виконкому та підрядних організацій, відповідальних за реалізацію інформаційної безпеки;

4.4.2 простого та захищеного обміну інформацією між усіма учасниками процесів діяльності;

4.4.3 стабільного функціонування інформаційних систем;

4.4.4 безпечного функціонування комп’ютерної техніки та мереж;

4.5 сприяння створенню атмосфери відкритості та підвищення ефективності внутрішньої комунікації;

4.6 відстеження, оцінювання та обробка ризиків інформаційних систем;

4.7 здійснення перевірок функціонування процесів системи інформаційної безпеки;

4.8 своєчасне виявлення змін критично важливих компонентів інформаційних систем, що виникають у результаті зовнішнього несанкціонованого впливу;

4.9 захист інформаційних ресурсів виконкому районної в місті ради від несанкціонованого доступу до даних, виявлення та запобігання витоку конфіденційної інформації.

Керуючий справами виконкому ***Олександр Гижко***

Додаток 7
до розпорядження голови
районної в місті ради
від 24.11.2021 № 345-р

Процедура
управління інформаційними активами
виконкому Довгинцівської районної в місті ради

І. Загальні вимоги

1.1. Відповідальність за активи

Для досягнення і підтримки в робочому стані, належного захисту організаційних активів усі активи повинні бути враховані і мати призначеного власника.

Усі активи повинні містити визначених власників, які нестимуть відповідальність за підтримання в робочому стані засобів управління. Реалізація конкретних засобів управління може бути делегована власником (за обставинами), але власник залишається відповідальним за належний захист активів.

1.2. Опис активів

Всі активи повинні бути чітко визначені. Опис усіх важливих активів складається і підтримується в робочому стані.

Виконком повинен виявити всі активи і документально підтвердити їх важливість. Опис активів має включати всю інформацію, необхідну для відновлення, включаючи тип активу, формат, місце розташування, дублюючу інформацію, інформацію про ліцензії, а також цінність для виконкому. Опис не повинен надмірно дублювати інші описи, але слід забезпечити, щоб його вміст було синхронізовано.

Крім того, власність і класифікація інформації повинні бути узгоджені і документально підтверджені для кожного з активів. На основі важливості активу повинні бути визначені його цінність для виконкому та категорія захисту, рівні захисту, співрозмірні з важливістю активів.

Існує багато типів активів, включаючи наступні:

- інформація: бази даних і файли даних, договори та угоди, системна документація, науково-дослідна інформація, настанови користувача, навчальний матеріал, процедури експлуатації або допоміжні процедури, плани забезпечення безперервності діяльності, заходи щодо нейтралізації несправності, контрольні журнали і архівована інформація;
- програмні активи: прикладні програми, системні програми, інструментальні засоби розробки і утиліти;
- фізичні активи: комп’ютерне обладнання, апаратура зв’язку, змінні носії інформації та інше обладнання;
- послуги: обробка даних і послуги зв’язку, загальні комунальні послуги, наприклад,опалення, електроенергія і кондиціювання повітря;

- працівники, їх кваліфікація, здібності та досвід;
- нематеріальні активи, такі як репутація і імідж виконкому.

Опис активів допомагає забезпечити їх результативний захист і також може бути необхідний для інших виробничих цілей, таких як техніка безпеки та охорона праці, страхування або фінансові причини (управління активами). Процес складання опису активів є важливою попередньою умовою управління ризиками.

1.3. Власність на активи

Уся інформація та активи, пов'язані із засобами обробки інформації, повинні перебувати у власності структурних підрозділів виконкому.

Власник активу повинен нести відповідальність за наступне:

- забезпечення того, щоб інформація та активи, пов'язані з засобами обробки інформації, були належним чином класифіковані;
- визначення і періодичний аналіз обмежень і класифікацій доступу, з урахуванням застосовуваної політики в галузі управління доступом.

Термін «власник» означає особу або об'єкт, які затвердили адміністративну відповідальність за управління виробництвом, розробкою, підтримкою в робочому стані, використанням та захистом активів. Термін «власник» не означає, що людина дійсно має будь-які права власності стосовно активу.

Власність може бути призначена на наступне:

- діловий процес;
- певний набір видів діяльності;
- певний набір даних.

1.4. Прийнятне використання активів

Правила прийнятного використання інформації та активів, пов'язаних із засобами обробки інформації, повинні бути визначені, документально підтверджені і реалізовані.

Усі службовці, підрядники та користувачі третіх сторін повинні слідувати правилам прийнятного використання інформації та активів, пов'язаних із засобами обробки інформації, включаючи наступні правила:

- правила використання електронної пошти та доступу до глобальної мережі Інтернет;
- принципи використання мобільних пристроїв, особливо для використання за межами приміщень виконкому.

Конкретні правила або вказівки повинні представлятися відповідним керівництвом. Службовці, підрядники та користувачі третіх сторін, що використовують або мають доступ до активів організації, повинні бути обізнані про межі для користування інформацією та активами виконкому, пов'язаними із засобами обробки інформації, а також ресурсами виконкому. Вони несуть відповідальність за користування будь-якими ресурсами з обробки інформації і за будь-яке таке користування, здійснене під їхню відповідальність.

1.5. Класифікація інформації

З метою визначення потреби в захисті, пріоритетів захисту та очікуваної ступені захисту при поводженні з інформацією вона має бути класифікована.

Інформація має різні ступені важливості і критичності. Деякі елементи можуть потребувати додаткового рівня захисту або спеціального поводження. Для визначення відповідного переліку рівнів захисту і повідомлення про потреби в заходах за спеціальним зверненням потрібно використовувати схему класифікації інформації.

Інформація повинна бути класифікована з погляду її значимості, відповідальності вимогам закону, конфіденційності та критичності для виконкому.

Класифікації та пов'язані з нею захисні засоби управління для інформації повинні враховувати потреби виконкому в поділі або обмеженні інформації, а також негативний вплив на діяльність виконкому, пов'язаний з такими потребами.

Керівні вказівки по класифікації повинні включати угоди про початкову класифікацію та повторну класифікацію з плином часу; відповідно до деякої попередньо визначеної політики в галузі управління доступом.

Власник активу повинен бути відповідальним за визначення класифікації активу, її періодичний аналіз і забезпечення її підтримки в актуальному стані.

Класифікація повинна враховувати ефект агрегації.

Слід приділити увагу числу категорій класифікації та вигодам, які потрібно отримати з їх використання. Надмірно складні схеми можуть стати громіздкими і неекономічними для використання або нездійсненними на практиці. Слід бути уважним при інтерпретації класифікаційних маркувань на документах з інших організацій, які можуть мати інші визначення для марку-вання з тим самим або аналогічним найменуванням.

Рівень захисту може бути оцінений шляхом аналізу конфіденційності, цілісності і доступності, а також будь-яких інших вимог для розглянутої інформації.

Інформація часто перестає бути важливою або критичною через певний період часу. Наприклад, коли інформація була зроблена загальновідомою. Ці аспекти повинні бути взяті до уваги, оскільки надмірна класифікація може привести до реалізації необов'язкових засобів управління, що дають в результаті додаткові витрати.

Розгляд документів з аналогічними вимогами захисту разом з призначенням рівнів класифікації може допомогти спростити завдання класифікації.

Класифікація інформації - це короткий спосіб визначити те, як належить поводитися з цією інформацією і як її потрібно захищати.

1.6. Маркування інформації та поводження з інформацією

У відповідності до схеми класифікації, прийнятої виконкомом, повинен бути розроблений і реалізований відповідний набір процедур для маркування інформації та поводження з інформацією.

Необхідно, щоб процедури для маркування інформації охоплювали інформаційні активи в фізичних та електронних форматах.

Вивід з систем, що містять інформацію, яка класифікується як важлива чи критична, повинен мати на собі відповідне класифікаційне маркування. Маркування має відображати класифікацію залежно від правил, установлених у пункті 1.5. Об'єкти, які потрібно взяти до уваги, включають надруковані звіти, екранні пристрої відображення, записані носії (наприклад, стрічки, диски, компакт-диски), електронні повідомлення і передані файли.

Для кожного класифікаційного рівня повинні бути визначені процедури поводження, включаючи захищену обробку, зберігання, передачу, розсекречення і знищення. Сюди також слід включити процедури послідовності турботи про збереження інформації та реєстрації будь-якої значимої події в системі захисту.

Угоди з іншими організаціями, які включають спільне використання інформації, повинні включати процедури для ідентифікації класифікації цієї інформації і для інтерпретації класифікаційного маркування інших організацій.

Маркування та захищене звернення з важливою інформацією є ключовою вимогою для заходів по спільному використанню інформації.

Фізичне маркування є звичайною формою маркування. Деякі інформаційні активи, наприклад, документи в електронній формі, не можуть бути помічені фізично, тому повинні бути використані електронні засоби маркування. Наприклад, сповіщувальне маркування може з'являтися на екрані або на пристрої відображення. Якщо маркування неможливо виконати, то можна застосувати інші засоби визначення класифікації, наприклад, за допомогою процедур або метаданих.

II. Ідентифікація та визначення цінності активів, визначення вартості впливу

2.1. Загальні положення

Щоб визначити цінність активу, спочатку необхідно ідентифікувати свої активи (на відповідному рівні деталізації).

Можна відрізнити два види активів:

• первинні активи:

- процеси та дії;
- інформація;

• активи підтримки (на які покладаються первинні елементи області застосування) всіх типів:

- апаратний засіб;
- програмне забезпечення;
- мережа;
- персонал;
- розміщення;
- організаційна структура.

2.2. Ідентифікація первинних активів

Діяльність в ідентифікації первинних активів (процеси, інформація) полягає в тому, щоб описати більш точно цю область застосування. Ця іденти-фікація процесів виконується представниками робочої змішаної групи (управ-лінці, фахівці з інформаційних систем і користувачі).

Зазвичай первинні активи - це основні процеси та інформаційна діяльні-сть в області застосування. Можна також розглядати інші первинні активи, такі як процеси всередині організації, які будуть більш відповідними для складання політики інформаційної безпеки або плану безперервності діяльності виконкому. Залежно від мети деякі дослідження не вимагатимуть вичерпного аналізування всіх елементів, складових області застосування. У таких випадках межі дослідження можуть бути обмежені ключовими елементами області застосування.

Первинні активи мають два типи:

1. Процеси (або підпроцеси) і дії, наприклад, процеси:

- втрата яких або деградація, позбавляють можливості виконувати завдання виконкому;
- які, якщо змінені, можуть суттєво вплинути на виконання завдань виконкому;
- які необхідні для виконкому, щоб виконати договірні, юридичні або регулюючі вимоги.

2. Інформація:

Більш широко первинна інформація включає головним чином:

- життєво важливу інформацію для здійснення діяльності виконкому;
- персональну інформацію, яка може бути визначена державою щодо права приватного життя;
- стратегічну інформацію для досягнення цілей, визначену стратегічними орієнтаціями;
- інформацію високої вартості, на збір, зберігання, обробку та передачу її потрібно багато часу і/або залучення значних фінансових витрат.

Після визначення процесів та інформації, які ідентифіковані як нечутливі, у кінцевому підсумку дослідження не треба ніякої визначеної класифікації. Це означає те, що навіть якщо такі процеси або інформація поставлені під загрозу, виконком буде виконувати свої завдання успішно.

Однак структурні підрозділи виконкому часто успадковують здійснення контролю, щоб захистити процеси та інформацію, ідентифіковану як чутливу.

2.3. Перелік та опис підтримки активів

Область застосування складається з активів, які повинні бути ідентифіковані та описані. У цих активів є вразливості, які є придатними для використання загрозами, які прагнуть послаблювати первин-ні активи області застосування (процеси та інформацію). Вони мають різні типи, приклад яких наведений у додатку 1.

2.4. Оцінка активу

Наступним кроком після ідентифікації активу потрібно узгодити шкалу, засновану на оцінці, за якою вона буде застосовуватися, і критерії для призначення місцезнаходження в цій шкалі для кожного активу.

Типові терміни, використані для якісної оцінки активів, включають слова, такі як: «незначний», «дуже низький», «низький», «середній», «високий», «дуже високий» і «критичний». Вибір і діапазон термінів, які підходять для виконкому, суворо залежить від потреб виконкому в безпеці, його розміру та інших специфічних факторів.

2.4.1. Критерії

Використовувані критерії, як підстава для того, щоб оцінити значення кожного активу, повинні бути виписані в однозначних термінах. Прийнятні критерії визначають, що значення активу включає свою оригінальну вартість, свою заміну, або вартість створення заново, або їх значення може бути абстрактним, наприклад, значення репутації виконкому.

Інша підстава для оцінки активів - збитки, понесені через втрату конфіденційності, цілісності та доступності. Така оцінка забезпечила б важливу розмірність елемента значенню активу на додаток до вартості заміни, заснованої на оцінках несприятливих наслідків для діяльності, які будуть випливати з інцидентів безпеки з прийнятим збігом обставин. Це дозволить розрахувати результати, які необхідні для визначення фактору оцінки ризику.

Багато активів протягом оцінки можуть приймати кілька значень в залежності від ситуації, в якій може опинитися актив. Кожне з призначених значень найбільш імовірно буде значно відрізнятися. Призначене значення може бути максимумом усіх можливих значень або може бути сумою деяких або всіма можливими значеннями. В кінцевому аналізі повинні бути ретельно визначені, оцінені або призначені значення для активів, оскільки кінцеве призначене значення виражається в ресурсах, які будуть витрачені для захисту активу.

Усі оцінки активу повинні бути приведені до загального значення. Це може бути зроблено за допомогою відповідних критеріїв. Критерії, які можуть використовуватися, щоб оцінити можливі наслідки через втрату конфіденційності, цілісності, доступності активів:

- порушення вимог законодавства та інших вимог;
- погіршення продуктивності;
- погіршення репутації;
- порушення, пов’язане з використанням персональних даних;
- загроза персональної безпеки;
- негативний вплив на приведення законів у життя;
- порушення конфіденційності;
- порушення громадського порядку;
- фінансова втрата;
- призупинення діяльності;
- загроза екологічної безпеки.

Для оцінки наслідків можуть бути використані інші підходи:

• призупинення обслуговування:
- неспроможність надати послугу;
• втрата довіри замовника:
- втрати довіри у внутрішній інформаційній системі;
- шкода репутації;
• руйнування внутрішньої працездатності:
- руйнування безпосередньо у виконкомі;
- додаткової внутрішньої вартості;
• руйнування працездатності третьої особи:
- руйнування у третіх осіб, які працюють з виконкомом;
- різноманітні типи ушкодження;
• порушення законів / інструкцій:
- неспроможність виконати юридичні зобов'язання;
• порушення умов контракту:
- неспроможність виконати договірні зобов'язання;
• небезпека для персоналу / користувальницької безпеки:
- небезпеки для персоналу організації та / або користувачів;
• атаки на приватне життя користувачів;
• фінансові втрати;
• фінансовій вартості для надзвичайної ситуації або відновлення в термінах:
- персоналу;
- обладнання;
- досліджень, звітів експертів;
• втрата товарів / грошових коштів / активів;
• втрата замовників, постачальників;
• судові позови і штрафи.
• втрата технологічної / технічної головної ролі;
• втрата ефективності / довіри;
• втрата технічної репутації;
• зниження ролі у веденні переговорів;
• індустріальні кризи;
• урядові кризи;
• звільнення;
• матеріальні збитки.

2.4.2. Шкала

Після встановлення критеріїв виконком має домовитися про шкалу оцінок, якою будуть користуватися всі структурні підрозділи. Перший крок полягає в виборі кількості рівнів, які будуть використовуватися. Немає жодних правил щодо кількості рівнів, які найбільш підходять. Більша кількість рівнів забезпечує більший рівень ступеня деталізації. Звичайно приймається будь-яке число рівнів від трьох (наприклад, низький, середній і високий рівень) до 10, яке може використовуватися сумісно з підходом виконкому щодо процесу, використовуваного для оцінки ризику в цілому. Виконком може визначити свої

власні межі для значень активу, як "низьке", "середнє" або "високе". Ці межі повинні бути оцінені згідно з обраними шкалами.

2.4.3. Залежності

Чим більш значущий актив у справі підтримки численних процесів, тим більше значення цього активу. Повинні бути ідентифіковані також залежності активів від процесів та інших активів, оскільки це може впливати на значення активів.

Наприклад, має бути збережена конфіденційність даних усюди по всьому життєвому циклу даних, на всіх стадіях, включаючи зберігання і обробку. Потреби безпеки зберігання даних і обробки програмою мають бути безпосередньо пов’язані зі значенням, що представляють конфіденційність даних, зберігання і обробку. Якщо процес покладається на цілісність відповідних даних, вироблених відповідно до програми, вхідні дані цієї програми повинні мати відповідну надійність. Цілісність інформації буде залежати від апаратних засобів і програмного забезпечення, використовуваного для її зберігання і обробки. Апаратні засоби будуть залежати від джерела живлення і можливо кондиціонування повітря. Таким чином, інформація про залежності допоможе ідентифікації загроз і особливо уразливості. Додатково, це допоможе переконувати, що активам надано істинне значення (через відносини залежності), таким чином, вказуючи відповідний рівень захисту.

Значення активів, від яких залежать інші активи, можуть бути змінені у таких випадках:

• якщо значення залежних активів (наприклад, даних) нижче або дорівнюють значенню активу, що розглядається (наприклад, програмне забезпечення), його значення остається тим же самим;

• якщо значення залежного активу (наприклад, дані) більше, то значення активу, який розглядають (наприклад, програмне забезпечення), має бути відповідно збільшене відповідно до:

- степеню залежності;
- значення інших активів.

Останнім кроком процесу є формування переліку активів із зазначенням їх значень щодо розкриття (збереження конфіденційності), модифікації (збереження цілісності, автентичності, спостережності), відсутності готовності і знищення (збереження доступності та надійності) і вартості заміни.

2.5. Оцінка впливу

Інцидент інформаційної безпеки може впливати на більше ніж один актив або тільки на частину активу. Вплив пов’язаний зі ступенем успіху інциденту. Як наслідок, є важлива відмінність між значенням активу і впливом, який наступає через інцидент. Впливом вважають наявність або безпосередній (експлуатаційний) ефект або майбутній (діловий) ефект, який включає фінансові та ринкові наслідки.

Безпосередній (експлуатаційний) вплив є прямим або непрямим.

Прямий вплив:

- фінансове значення заміни втраченого активу (його частини);
- вартість придбання, конфігурації і інсталяції нового активу або резервної копії;
- вартість призупинених операцій через інцидент до відновлення послуги, наданої активом (-ами);
- яке призводить до порушення правил інформаційної безпеки.

Непрямий вплив:

- альтернативні витрати (фінансові ресурси повинні замінити або виправити актив, який буде використовуватися в іншому місці);
- вартість перерваних операцій;
- потенційно неправильне вживання інформації отриманої через порушення правил безпеки;
- порушення встановлених законом або регулюючих зобов'язань;
- порушення норм моральної поведінки.

2.6. Методика оцінки вартості

На початковому етапі необхідно сформувати інформаційні активи як об'єкт обліку та оцінки. Алгоритм оцінки наявних інформаційних активів включає в себе їх опис за наступними категоріями:

- людські ресурси;
- інформаційні активи (відкрита і конфіденційна інформація);
- програмні ресурси (програмні продукти, бази даних, корпоративні сервіси, КАІ-Докуметнообіг, Банк-клієнт та інші, а також залежне апаратне зfбезпечення);
- фізичні ресурси (сервера, робочі станції, мережеве та телекомунікаційне обладнання, в тому числі мобільні пристрої);
- сервісні ресурси (електронна пошта, веб-ресурси, онлайн-сховища, канали передачі даних тощо);
- приміщення (в яких обробляється і зберігається інформація).

Далі експертна комісія, яка формується за розпорядженням голови і складається з вузькокваліфікованих фахівців - експертів, проводить детальну категоризацію наявної інформації, тобто виділення інформації, яка захищається, з усього обсягу інформаційних активів, а далі з категорії інформаційних активів, які захищаються - виділення конкретно цінної конфіденційної інформації.

Категоризація полягає у визначенні рівня цінності інформації, її критичності. Підкритичними розуміється ступінь впливу інформації на ефективність функціонування господарських процесів виконкому.

Наприклад, визначення цінності інформації може бути відображено в таблиці 1, де сума балів, розташованих на перетині стовпців і рядків таблиці, вказує на цінність інформації в цілому для виконкому, що включає в себе вид інформації з точки зору обмеженості доступу до неї і критичність інформації для компанії.

Таблиця 1
Визначення цінності інформації

Параметр/значення	***Критичність інформації***		
Цінність виду інформації	***Критична (3 бали)***	***Суттєва (2 бали)***	***Незначна (1 бал)***
Суворо конфіденційна (4 бали)	7	6	5
Конфіденційна (3 балла)	6	5	4
Для внутрішнього користування (2 балла)	5	4	3
Відкрита (1 балл)	4	3	2

Можна використовувати галузевий диференційований підхід: присвоїти параметру цінності інформації певне вагове значення для визначення рівня значущості ресурсу з точки зору його участі в діяльності виконкому. Наприк-лад, можна визначити коефіцієнт цінності різних категорій інформації, відображених у таблиці 2.

Таблиця 2
Коефіцієнт цінності інформації

Категорія інформації	***Відкрита інформа-ція***	***Конфіденційна інформація***			
		Управлін-ська	***Технологіч-на***	***Фінансова, бухгалтер.***	***Персона-льні дані***
Коефіцієнт цінності	1	1,4	1,3	1,2	1,1

Також є ще один підхід до визначення цінності інформації (в результаті можливості поповнення втрат у разі реалізації загроз) в співвідношенні з імовірністю прояви загроз (таблиця 3).

Таблиця 3
Визначення втрат і ймовірності реалізації загроз

Втрати	***Ймовірність реалізації загрози***		
	Несуттєва, менше 1%	***Суттєва, від 1% до 10%***	***Висока, більше 10%***
Незначні (менше 1% вартості організації)	1	2	2
Значні (від 1% до 10%)	2	2	2
Критично високі (більше 10%)	2	3а*	3б*

*Ризики підкатегорії 3б неприйнятні для виконкому і повинні бути нейтралізовані в будь-якому випадку, навіть якщо для цього необхідно пере-будувати всі процеси.

У підсумку оцінюється сумарна значущість інформації і застосовуваних інформаційних технологій у діяльності виконкому. Показник може мати приблизну якісну оцінку - «дуже значимо», «істотно значимо», «мало значимо», «не значимо». А також приблизну кількісну оцінку - процентну (на скільки % діяльність виконкому залежить від використовуваної інформації).

Експертними методами з застосуванням математичних методів також вираховується «суб'єктивна» і «об'єктивна» ймовірність тієї чи іншої загрози, загальне значення якої враховується при складанні таблиці (таблиця 4).

Таблиця 4.
Перетворення ймовірності реалізації загрози до щорічної частоти

Частота	***Ймовірність виникнення загрози за визначений період***	***Рівень ймовірності***
0,05	загроза практично ніколи не реалізується	дуже низький рівень
0,6	приблизно 2-3 рази на 5 років	дуже низький рівень
1	приблизно 1 раз на рік та менше (180<У>366 (днів))	низький рівень
2	приблизно 1 раз на півроку (90<У<180 (днів))	низький рівень
4	приблизно 1 раз на 3 місяці (60<У<90 (днів))	середній рівень
6	приблизно 1 раз на 2 місяці (30<У<60 (днів))	середній рівень
12	приблизно 1 раз на місяць (15<У<30 (днів))	високий рівень
24	приблизно 2 рази на місяць (7<У<15 (днів))	високий рівень
52	приблизно 1 раз на тиждень (1<У<7 (днів))	дуже високий рівень
365	щоденно (1<У<24 (годин))	дуже високий рівень

Для грошового вираження вартості доцільно розглядати цінність інформаційних ресурсів як з точки зору асоційованих з ними можливих фінансових втрат (яке виражається в грошовому еквіваленті), так і з точки зору шкоди репутації виконкому (непрямих фінансових втрат), дезорганізації її діяльності, нематеріальної шкоди від розголошення конфіденційної інформації і т.д. Таким чином, цінність активу визначається експертами шляхом оцінки ступеня можливого нанесення збитку виконкому при неправомірному використанні розглянутої інформації (тобто в разі порушення його конфіденційності, цілісності або доступності).

Щоб уникнути витрат на ліквідацію наслідків, необхідно аналізувати можливість реалізації загроз безпеці виданих інформаційних активів виконкому. Для експертної оцінки можливого збитку від реалізації загроз використо-

вуються наступні категорії: вартість відновлення та ремонту обчислювальної техніки; мережі та іншого обладнання; судові витрати; втрата продуктивності праці; втрати, пов’язані з простоєм і виходом з ладу обладнання.

В управлінні ризиками інформаційної безпеки для оцінки вартості інформації застосовується метод очікуваних втрат, що показує можливі втрати організації в результаті невідповідних заходів захисту інформації. Виробляється обчислення рівня ризику, тобто показника можливих втрат (збитків) враховуючи такі аспекти, як імовірність і частота прояву тієї чи іншої загрози протягом року, можливий збиток від її реалізації, ступінь уразливості інформації.

Сумарна величина економічного збитку розділена на кілька категорій:

- вартість заміни, відновлення та ремонту обчислювальної техніки, мережі та іншого обладнання;
- втрата продуктивності (простій).

Керуючий справами виконкому ***Олександр Гижко***

Додаток
до Процедури управління
інформаційними активами
виконкому Довгинцівської
районної в місті ради

Типовий перелік активів

Апаратні засоби

Апаратний тип складається з усіх фізичних елементів, що підтримують процеси.

Апаратура обробки даних (активна)

Устаткування для автоматичного оброблення інформації.

Мобільне обладнання

Переносне комп'ютерне обладнання (ноутбук, кишеньковий комп'ютер).

Установлене обладнання

Комп'ютерне обладнання використовується в приміщенні виконкому (сервер, мікрокомп'ютер, використовуваний як робоча станція).

Пристрої обробки периферії

Обладнання, підключене з комп'ютером через комунікаційний порт (послідовний, паралельний і т.д.) для того, щоб ввести, перенаправити або передавати дані (принтер, змінний дисковод).

Носії даних (пасивні)

Носії для того, щоб зберігати дані або функції.

Електронні засоби

Засоби зберігання інформації, які можуть бути підключені до комп'ютерної мережі або мережі зберігання даних. Незважаючи на їх компактний розмір, ці носії можуть містити велику кількість даних. Вони можуть використовуватися зі стандартним обчислювальним обладнанням (гнучкий диск, CD-ROM, резервний картридж, змінний апаратний диск, ключі захисту пам'яті).

Інші носії

Статичні, неелектронні носії, що містять дані (папір, слайд, діапозитив, документація, факс).

Програмне забезпечення

Програмне забезпечення складається з усіх програм, які сприяють обробці даних.

Операційна система

Всі програми комп'ютера, що становить операційне ядро від котрого включаються всі інші програми (служби або програми). Операційна система включає ядро і основні функції або служби. Залежно від архітектури операційна система може бути монолітною або складена з мікроядра і ряду системних служб. Основні елементи операційної системи - всі служби менеджменту облад-нанням (центральний процесор, пам'ять, диск і мережеві інтерфейси), завдання або менеджмент процесів і користувальницькі служби менеджменту правами.

Програмне забезпечення сервісу, обслуговування або забезпечення

Програмне забезпечення характеризується фактом того, що воно є доповненням служби операційної системи і не безпосередньо сервісів користувачів або додатків (навіть при тому, що це є зазвичай основним або навіть обов'язко-вим для глобальної експлуатації інформаційної системи).

Пакет програмного або стандартного програмного забезпечення

Стандартне програмне забезпечення або пакет програмного забезпечення – це сукупність програм системи обробки інформації і програмних документів, необхідних для експлуатації цих програм.

Додатки

Стандартні додатки – це комерційне програмне забезпечення, спроектоване, щоб дати користувальницький прямий доступ до служб і функцій, яких вони вимагають від їх інформаційної системи. Є дуже широке коло теоретично безмежне поле застосування (програмне забезпечення облікових записів, специфічне програмне забезпечення, адміністративне програмне забезпечення тощо)

Специфічні додатки - програмне забезпечення, в якому різні аспекти (передусім підтримка, обслуговування, оновлення і т.д.) були спеціально розроблені, щоб надати прямий користувальницький доступ до служб і функцій, які потрібні користувачеві від їх інформаційної системи. Є дуже широке, теоретично необмежене поле застосування (менеджмент рахунків клієнтів телекомунікаційних операторів в реальному часі і моніторинг додатків в реальному часі).

Мережа

Мережевий тип складається з усіх пристроїв передачі даних, що використовуються, щоб зв'язати кілька фізично віддалених комп'ютерів або елементів інформаційної системи.

Способи передачі та підтримки

Передача інформації та носів даних або обладнання характеризуються головним чином відповідно до фізичних і технічних характеристик обладнання (точка-точка, широковіщальне) і відповідно до протоколів комунікації (лінія зв'язку або мережу - рівні з'єднання 2 і 3 з 7-ми рівневої OSI-моделі відкритих систем) (Ethernet, Gigabit Ethernet, асиметрична цифрова абонентська лінія (ADSL), бездротові специфі-кації протоколу (наприклад, WiFi 802.11), технологія Bluetooth, FireWire.

Пасивне чи активне обладнання передачі

Цей підтип включає всі пристрої, які не є логічно завершеними в телекомунікаціях (система технічного зору на інформаційну систему), але є проміжними або передавальними пристроями. Передача характеризована відповідно до підтримуючих мережевих протоколів комунікації.

На додаток до основної функції передачі вони часто включають маршрутизацію і/або функції та служби фільтрації, використовуючи комутатори комунікації та маршрутизатори з фільтрами. Ними можна часто управляти дистанційно і зазвичай вони здатні до генерації журналів (міст, маршрутизатор, концентратор, автоматичний комутатор каналів).

Комунікаційні інтерфейси

Комунікаційні інтерфейси підключені до оброблювальних пристроїв для обробки, але характеризуються носіями і підтримуваними протоколами, будь-якої встановленої фільтрації, веденням журналів або функціями попередження, потужностями та вимогами можливого віддаленого адміністрування (пакетний радіозв'язок загального призначення (GPRS), адаптер Ethernet).

Персонал

Тип персоналу складається з усіх груп людей, залучених до інформацій-ної системи.

Особи, які приймають рішення

Особи, які приймають рішення - власники первинних активів (інформації та функціоналу) вище виконавче керівництво.

Користувачі

Користувачі - персонал, який обробляє чутливі елементи в середовищі їх діяльності та у якого є спеціальна відповідальність у цьому відношенні. У них можуть бути спеціальні права доступу до інформаційної системи, щоб виконувати їх щоденні завдання (управляючі персоналом, фінансами тощо).

Штатні співробітники експлуатації / обслуговування

Це - персонал, що відповідає за експлуатацію та підтримку інформаційної системи.

Розробники

Розробники відповідають за розробку додатків організації. Вони мають доступ до частини інформаційної системи з правами високого рівня, але не роблять дії на виробничих даних (розробники ділових додатків, програмного забезпечення).

Територія

Територія включає всю площу, яка містить сфери діяльності або частина цієї сфери та фізичні засоби, необхідні для цієї роботи.

Приміщення

Це місце обмежене периметром виконкому.

Зона

Зона сформована фізичним захисним кордоном, який формує поділ в межах приміщення організації. Зона утворюється фізичними бар'єрами навколо інфраструктур обробки інформації виконкому.

Основні служби

Всі служби, необхідні для роботи обладнання виконкому.

Комунікація

Служби передачі даних і устаткування забезпечення операторів (телефонна лінія, установчі АТС з вихідним і вхідним зв'язком, внутрішні телефонні мережі).

Комунальний сервіс

Сервіси і засоби (джерела і електропроводка) вимагаються для того, щоб забезпечити живлення обладнання інформаційних технологій і периферійних пристроїв (низьковольтні джерела живлення напруги, інвертор, головний вузол каналу електричної мережі).

Водопостачання.

Вивіз відходів.

Служби та засоби (обладнання, контроль) для охолодження й очищення повітря (канали водного охолодження, кондиціонери).

Організація

Організацію характеризують типи організаційної структури, які складаються з усіх структур персоналу і процедур, керуючих цими структурами.

Проектна або системна організація

Це стосується організації, встановленої для окремого проекту або сервісу (розробка нового прикладного проекту, проект міграції інформаційної системи).

Субпідрядники / постачальники / виробники.

Це організації, які надають виконкому сервіс або ресурси і пов’язані з нею відповідно до контракту (компанія управління коштами, аутсорсінг-компанія, консультаційна компанія).

Додаток 8
до розпорядження голови
районної в місті ради
від 24.11.2021 № 345-р

Реєстр
інформаційних активів виконкому Довгинцівської районної в місті ради

№ з/п	***Активи***	***Клас активу***	***Розпорядник активу***	***Рівні доступу до активу***
Імідж та репутація				
1	Імідж та репутація	Імідж та репутація	Структурні підрозділи та галузеві спеціалісти	Повний
Персонал				
2	Голова районної в місті ради	Персонал	Голова районної в місті ради	Обмежений
3	Заступник голови районної в місті ради, заступники голови районної в місті ради з питань діяльності виконавчих органів, керуючий справами виконкому районної в місті ради	Персонал	Заступник голови районної в місті ради, заступники голови районної в місті ради з питань діяльності виконавчих органів, керуючий справами виконкому	Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
			районної в місті ради	
4	Персонал	Персонал	Структурні підрозділи та галузеві спеціалісти	Обмежений
Інформація				
5	Ордера на виконання земляних робіт	Інформація	Відділ з питань благоустрою, транспорту та житла	Обмежений
6	Протоколи засідань громадської комісії з житлових питань	Інформація		Обмежений
7	Журнал обліку видачі ордерів на житлову площу (виданих викон-комом районної в місті ради, підприємствами та викон-комами інших районів міста Кривого Рогу)	Інформація		Обмежений
8	Журнал обліку видачі ордерів на службові жилі приміщення	Інформація		Обмежений
9	Облікові справи осіб, які перебувають на квартирному обліку для поліпшення житлових умов	Інформація		Обмежений
10	Книга обліку осіб, які перебувають на квартирному обліку для поліпшення житлових умов при виконкомі районної в місті ради	Інформація		Обмежений
11	Документація з цивільного захисту населення і території району від надзвичайних ситуацій техногенного характеру	Інформація	Відділ з питань мобілізаційної роботи, надзви-чайних ситуацій та цивільного захисту насе-лення	Обмежений
12	Документація з мобілізації та мобілізаційної роботи, взаємодії та координаційної діяльності правоохоронних органів та громад-ських формувань з охорони громадського порядку	Інформація	Відділ з питань мобілізаційної роботи,	Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
			надзвичайних ситуацій та цивільного захисту населення	
13	Автоматична система «КАІ-Документообіг. Електронний документообіг»	Інформація	Загальний відділ	Обмежений
14	Автоматична система «КАІ-Документообіг. Звернення гро-мадян»	Інформація		Обмежений
15	Номенклатура справ	Інформація		Обмежений
16	Листування з обласною державною адміністрацією з питань основної діяльності	Інформація		Обмежений
17	Листування з обласною радою з питань основної діяльності	Інформація		Обмежений
18	Листування з міським головою, його заступниками, керуючою справами, структурними підрозділами виконкому міськради з основних питань діяльності	Інформація		Обмежений
19	Протоколи засідань виконкому районної в місті ради та документи до них	Інформація		Обмежений
20	Протоколи сесій районної в місті ради та документи до них	Інформація		Обмежений
21	Розпорядження голови районної в місті ради	Інформація		Обмежений
22	Журнал обліку бланків суворої звітності	Інформація		Обмежений
23	Листування з організаціями, установами, підприємствами з питань роботи промислових підприємств, надання послуг, випуску товарів народного вжитку	Інформація		Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
24	Листування з організаціями з питань будівництва, благоустрою та утримання житлового та комунального фонду	Інформація		Обмежений
25	Листування з питань санітарного стану та екології на підпри-ємствах району	Інформація		Обмежений
26	Листування з питань роботи радіо, телефонної мережі, електрифікації, транспорту, ремонту і експлуатації	Інформація		Обмежений
27	Листування з організаціями з питань діяльності релігійних громад	Інформація		Обмежений
28	Листування з питань роботи державної і комерційної торгівлі, громадського харчування та побутового обслуговування, про експлуатацію і надання приміщень організації, здавання й приймання будівель в оренду	Інформація		Обмежений
29	Листування з питань охорони здоров’я та соціального захисту населення	Інформація		Обмежений
30	Листування з питань роботи закладів освіти, дошкільних закладів, організації літнього відпочинку дітей	Інформація		Обмежений
31	Листування з організаціями з питань діяльності закладів культури та спорту	Інформація		Обмежений
32	Листування з правоохоронними органами, територіальними центрами комплектування та соціальної підтримки, самостійними державними пожежними частинами з питань основної діяльності	Інформація		Обмежений
33	Листування з питань роботи добровільних громадських організацій та партій	Інформація		Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
34	Листування з питань фінансової, індивідуально-трудової та кооперативної діяльності	Інформація		Обмежений
35	Листування з банками, друкарнями, редакціями, організаціями з адміністративно-господарських питань	Інформація		Обмежений
36	Звернення (пропозиції, заяви і скарги) громадян з питань особистого характеру та листування про їх перевірку	Інформація		Обмежений
37	Списки дітей пільгових категорій, рекомендованих для оздор-овлення і відпочинку	Інформація	Відділ у справах сім'ї, молоді та спорту	Обмежений
38	Банк даних багатодітних сімей по району м.Кривого Рогу	Інформація		Обмежений
39	Список депутатів	Інформація	Організаційний відділ	Обмежений
40	Структура органів самоорганізації населення	Інформація		Обмежений
41	Дислокація органів самоорганізації населення	Інформація		Обмежений
42	Плани роботи районної в місті ради та її виконавчого комітету на місяць, квартал, півріччя	Інформація		Обмежений
43	АІС «Місцеві бюджети рівня міста, району»	Інформація	Фінансовий відділ	Обмежений
44	АІС «Соціальні виплати»	Інформація		Обмежений
45	База даних Єдиної інформаційно-аналітичної системи «Діти» (ЄІАС «Діти»)	Інформація	Служба у справах дітей	Обмежений
46	Списки релігійних громад району, політичних партій району, громадських організацій району та копії їх установчих документів	Інформація	Відділ з питань внутрішньої політики, взаємодії із засобами масової інформації та промоцій	Обмежений
47	Паспорт району	Інформація		Обмежений
48	Офіційний вебсайт виконкому районної в місті ради в мережі Інтернет (http://www.dlgr.gov.ua)	Інформація	Відділ інформаційних	Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
			технологій	
49	Списки дітей і підлітків шкільного віку на навчальний рік	Інформація	Відділ освіти	Обмежений
50	Списки дітей з інвалідністю, які навчаються в загальноосвітніх закладах	Інформація		Обмежений
51	Журнал протоколів засідань адміністративної комісії	Інформація	Секретар адміністра-тивної комісії	Обмежений
52	Програма в системі ЕМСКП від НОВА-КОМ	Інформація	Відділ бухгал-терського обліку	Обмежений
53	База даних M.E.DOC	Інформація		Обмежений
54	Клієнтське програмне забезпечення «ПриватБанк»	Інформація		Обмежений
55	База даних прикладного програмного засобу «Фіндоку-менти» МережаМ (формування на електронних та папе-рових носіях зведених кошторисів, розподілів, зобов’язань і платіжних дору-чень по державному та місцевому бюджетах)	Інформація		Обмежений
56	Документація службових розслідувань стосовно осіб, уповноважених на виконання функцій держави або місцевого само-врядування	Інформація	Головний спеціаліст з питань взаємодії з правоохоронними органами та запобігання корупції	Обмежений
57	Документація спеціальних перевірок відомостей щодо осіб, які претендують на зайняття посад, пов’язаних із виконанням функцій держави або місцевого самоврядування	Інформація		Обмежений
58	Документація конкурсних торгів	Інформація	Відділ економіки та промисловості	Обмежений
59	Документи (програми, анкети, схеми, звіти, висновки тощо) щодо запровадження системи управління якістю	Інформація		Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
60	База даних призначення і надання населенню компенсації додаткових витрат на оплату комунальних послуг в умовах підвищення цін і тарифів на послуги	Інформація	Управління праці та соціального захисту населення	Обмежений
61	База даних системи автоматизованої діяльності служб житлових субсидій (НАШ ДІМ)	Інформація		Обмежений
62	База даних автоматизованої системи обробки пенсійної документації (АСОПД/КОМ-ТЕХ) та Asopdsoc	Інформація		Обмежений
63	База даних програмного забезпечення M.E.DOC	Інформація		Обмежений
64	База даних Єдиного державного автоматизованого реєстру осіб, які мають право на пільги (ЄДАРП)	Інформація		Обмежений
65	Методичні рекомендації, правила, положення, надіслані департаментом соціального захисту населення Дніпропетровської обл-держадміністрації	Інформація		Обмежений
66	Накази начальника управління з основної діяльності	Інформація		Обмежений
67	Посадові інструкції	Інформація		Обмежений
68	Журнал реєстрації письмових звернень громадян з питань особистого характеру	Інформація		Обмежений
69	Книги реєстрації вхідної, вихідної документації, вхідних та вихідних телефонограм	Інформація		Обмежений
70	Журнали, реєстрації прийому громадян з особистих питань керівниками управління	Інформація		Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
71	Протоколи оперативних нарад при керівнику управління	Інформація		Обмежений
72	Документи (листування, доповідні записки, акти обстежень) відповідей про стан розгляду пропозицій, заяв та скарг громадян	Інформація		Обмежений
73	Листування з підприємствами, установами, організаціями з питань основної діяльності (вхідна та вихідна кореспонденція)	Інформація		Обмежений
74	Листування з виконкомом Криворізької міської ради з основних питань діяльності управління	Інформація		Обмежений
75	Журнал реєстрації наказів з основної діяльності управління	Інформація		Обмежений
76	Журнал обліку зберігання печаток та штампів	Інформація		Обмежений
77	Номенклатура справ управління	Інформація		Обмежений
78	Звіти щодо стану призначення та виплати одержувачам дер-жавних соціальних допомог, компенсацій, субсидій: річні, квартальні, місячні	Інформація		Обмежений
79	Протоколи засідань комісії виконкому районної у місті ради з вирішення питань, пов’язаних з наданням населенню пільг, субсидій на житлово-комунальні послуги та державної соціальної допомоги малозабезпеченим сім’ям	Інформація		Обмежений
80	Журнал реєстрації прийому заяв та документів для призначення усіх видів соціальної допомоги	Інформація		Обмежений
81	Журнал обробки заяв (особових справ)	Інформація		Обмежений
82	Журнал обліку справ, переданих до архіву	Інформація		Обмежений
83	Журнали реєстрації заяв громадян, які постраждали внаслідок Чорнобильської катастрофи, на санаторно-курортне лікування категорій 1, 2, 3	Інформація		Обмежений
84	Журнал реєстрації заяв на санаторно-курортне лікування дітей, які постраждали внаслідок Чорнобильської катастрофи	Інформація		Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
85	Журнал реєстрації заяв на санаторно-курортне лікування дітей, які постраждали внаслідок Чорнобильської катастрофи, з батьками	Інформація		Обмежений
86	Журнал видачі путівок громадянам, які постраждали внаслідок Чорнобильської катастрофи	Інформація		Обмежений
87	Звіти з питань забезпечення громадян, які постраждали внаслідок Чорнобильської катастрофи, санаторно-курортними путівками	Інформація		Обмежений
88	Особові справи одержувачів державних соціальних допомог, компенсацій та субсидій	Інформація		Обмежений
89	Журнал обліку заяв та заяви ветеранів війни, які бажають отримати путівки на санаторно-курортне лікування	Інформація		Обмежений
90	Журнал обліку заяв осіб з інвалідністю, які бажають отримати путівки на санаторно-курортне лікування	Інформація		Обмежений
91	Журнал обліку заяв та заяви осіб з інвалідністю загального захворювання, які бажають отримати путівки на санаторно-курортне лікування	Інформація		Обмежений
92	Журнал реєстрації заяв на забезпечення технічними та іншими засобами реабілітації	Інформація		Обмежений
93	Журнал обліку заяв громадян щодо направлення їх до будинку-інтернату на постійне місце проживання	Інформація		Обмежений
94	Журнал реєстрації заяв інвалідів, законних представників дітей з інвалідністю на забезпечення автомобілями безкоштовно або на пільгових умовах	Інформація		Обмежений
95	Книга обліку видачі путівок в санаторії	Інформація		Обмежений
96	Журнал обліку надання компенсацій на бензин, ремонт та технічне обслуговування автомобілів, транспортні видатки	Інформація		Обмежений
97	Особові справи осіб з інвалідністю – отримувачів компенсацій на бензин, ремонт та технічне обслуговування автомобілів	Інформація		Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
98	Журнал обліку виплат компенсацій по санаторно-курортному лікуванню осіб з інвалідністю та особисті заяви	Інформація		Обмежений
99	Журнал реєстрації заяв і заяви осіб з інвалідністю та непрацюючих малозабезпечених осіб на отримання матеріальної допомоги	Інформація		Обмежений
100	Особові справи громадян, які перебувають під опікою чи піклуванням	Інформація		Обмежений
101	Журнал обліку заяв громадян району на обслуговування у відділенні організації надання адресної натуральної та грошової допомоги КУ «Територіальний центр соціального обслуговування (надання соціальних послуг) у Довгинцівському районі»	Інформація		Обмежений
102	Журнал реєстрації заяв громадян району на обслуговування КУ «Територіальний центр соціального обслуговування (надання соціальних послуг) у Довгинцівському районі»	Інформація		Обмежений
103	Журнал реєстрації заяв для встановлення статусу згідно з законами України «Про статус ветеранів війни, гарантії їх соці-ального захисту» та «Про жертви нацистських переслідувань», заяви з відповідними пакетами документів	Інформація		Обмежений
104	Журнал обліку видачі бланків суворої звітності (пільгові посвідчення та\або вкладки): - «інвалід війни» - «учасник війни» - член сім'ї загиблого (померлого) ветерана війни»	Інформація		Обмежений
105	Журнал обліку видачі бланків суворої звітності – листів-талонів на пільговий проїзд ветеранам війни	Інформація		Обмежений
106	Журнал реєстрації видачі довідок про перебування на обліку в Єдиному державному автоматизованому реєстрі осіб, які мають право на пільги	Інформація		Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
107	Журнал реєстрації особових справ громадян пільгової категорії	Інформація		Обмежений
108	Особові справи громадян пільгової категорії	Інформація		Обмежений
109	Журнал реєстрації заяв пільговиків по наданню пільг на тверде паливо готівкою	Інформація		Обмежений
110	Журнал реєстрації заяв пільговиків по наданню пільг на скраплений газ готівкою	Інформація		Обмежений
111	Журнал реєстрації заяв родичів померлих учасників бойових дій та інвалідів війни для отримання компенсації на поховання	Інформація		Обмежений
112	Особові справи родичів померлих учасників бойових дій та інвалідів війни для отримання компенсації на поховання	Інформація		Обмежений
113	Журнал реєстрації повідомлень про реєстрацію смерті громадян, наданих до відома органами МВС	Інформація		Обмежений
114	Повідомлення про реєстрацію смерті громадян району міста Кривого Рогу	Інформація		Обмежений
115	Книга обліку черги на виконання безоплатних капітальних ремонтів житлових будинків і квартир, що перебувають у власності осіб, яким надаються пільги згідно із законами України «Про статус ветеранів війни, гарантії їх соціального захисту», «Про жертви нацистських переслідувань» та «Про основні засади соціального захисту ветеранів праці та інших громадян похилого віку в Україні»	Інформація		Обмежений
116	Книга обліку житлових будинків і квартир, що перебувають у власності осіб, яким надаються пільги згідно із законами України «Про статус ветеранів війни, гарантії їх соціального захисту», «Про жертви нацистських переслідувань» та «Про основні засади соціального захисту ветеранів праці та інших громадян похилого віку в Україні», в яких проведено такий ремонт	Інформація		Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
117	Особові рахунки одержувачів соціальних допомог	Інформація		Обмежений
118	Журнал обліку прийому інформації електронною поштою	Інформація		Обмежений
119	Журнал реєстрації довідок про отримання (не отримання) допомог та компенсацій	Інформація		Обмежений
120	Журнал реєстрації виплатних документів	Інформація		Обмежений
121	Звіти про нарахування на загальнообов'язкове державне пенсійне страхування за деякі категорії застрахованих осіб	Інформація		Обмежений
122	Рішення, протоколи засідань комісії виконкому районної в місті ради з вирішення питань, пов'язаних з наданням матеріальної допомоги мешканцям району у зв'язку з похованням деяких категорій осіб та скрутним матеріальним становищем	Інформація		Обмежений
123	Журнал реєстрації особистих звернень громадян до соціального інспектора	Інформація		Обмежений
124	Журнал реєстрації виявлених порушень та стану відшкодування надміру нарахованих коштів	Інформація		Обмежений
125	Журнал реєстрації запитів та відповідей до установ, організацій та підприємств для перевірок довідок про доходи	Інформація		Обмежений
126	Журнал реєстрації перевірок цільового використання коштів допомоги при народженні дитини	Інформація		Обмежений
127	Журнал реєстрації актів обстеження матеріально-побутових умов проживання сім'ї на матеріальну допомогу	Інформація		Обмежений
128	Журнал реєстрації особових справ одержувачів усіх видів державної соціальної допомоги які перевіряються щодо правильності призначення допомоги	Інформація		Обмежений
129	Журнал реєстрації актів обстеження матеріально-побутових умов проживання сім'ї та особових справ одержувачів субсидій з зазначенням тих, які розглядаються комісійно	Інформація		Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
130	Журнал реєстрації судових справ та особові справи отримувачів допомог, що наявні в провадженні районного суду	Інформація		Обмежений
131	Реєстр колективних договорів району м. Кривого Рогу	Інформація		Обмежений
132	Документи (довідки, доповідні записки, звіти, листи) про виконання пропозицій за результатами обстежень, перевірок, запитів відділу праці та соціально-трудових відносин	Інформація		Обмежений
133	Свідоцтва про Державну реєстрацію юридичної особи	Інформація		Обмежений
134	Виписка з Єдиного реєстру юридичних осіб та фізичних осіб-підприємців	Інформація		Обмежений
135	База даних інформаційної системи «Картка»	Інформація	Відділ з питань кадрової роботи	Обмежений
136	Розпорядження голови районної в місті ради з кадрових питань (особового складу)	Інформація		Обмежений
137	Розпорядження голови районної в місті ради про короткострокові відрядження	Інформація		Обмежений
138	Розпорядження голови районної в місті ради про надання щорічних оплачуваних відпусток та відпусток у зв’язку з навчанням	Інформація		Обмежений
139	Положення про структурні підрозділи виконкому районної в місті ради, та зміни до них (копії)	Інформація		Обмежений
140	Особові справи працівників виконкому районної в місті ради	Інформація		Обмежений
141	Особові картки працівників (у тому числі тимчасових та працюючих за сумісництвом)	Інформація		Обмежений
142	Протоколи засідань конкурсних комісій із заміщення вакантних посад, обрання на посаду	Інформація		Обмежений
143	Трудові книжки працівників виконкому районної в місті ради	Інформація		Обмежений
144	Перелік розпоряджень голови районної в місті ради з кадрових питань (особового складу)	Інформація		Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
145	Перелік розпоряджень голови районної в місті ради про короткострокові відрядження	Інформація		Обмежений
146	Перелік розпоряджень голови районної в місті ради про надання щорічних оплачуваних відпусток та відпусток у зв'язку з навчанням	Інформація		Обмежений
147	Журнал обліку руху особових справ посадових осіб виконкому районної в місті ради	Інформація		Обмежений
148	Журнал приймання працівників (у тому числі тимчасових)	Інформація		Обмежений
149	Журнал переміщення працівників (у тому числі тимчасових)	Інформація		Обмежений
150	Журнал звільнення працівників (у тому числі тимчасових)	Інформація		Обмежений
151	Журнал обліку видачі трудових книжок і вкладок до них	Інформація		Обмежений
152	Статистичні (річні) звіти з кадрових питань	Інформація		Обмежений
153	Документи (нормативи чисельності, типові структури апарату, аналітичні таблиці, розрахунки, доповіді, довідки) про вдосконалення структури виконкому районної в місті ради	Інформація		Обмежений
154	Документи (протоколи, подання, анкети, акти тощо) про встановлення персональних окладів, надбавок, доплат	Інформація		Обмежений
155	Посадові та робочі інструкції працівників виконкому районної в місті ради	Інформація		Обмежений
156	Документи (акти, постанови, рішення, довідки, доповідні та пояснювальні записки, висновки, листи) службових розслідувань	Інформація		Обмежений
157	Документи (звіти, довідки, висновки, доповідні записки) про переведення працівників на скорочений робочий день або неповний робочий тиждень	Інформація		Обмежений
158	Документи (плани, звіти, копії наказів, листи) про стажування	Інформація		Обмежений
159	Списки кандидатів на висування за посадою (резерв)	Інформація		Обмежений
160	Протоколи засідань, рішення атестаційної комісії	Інформація		Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
161	Документи (характеристики, атестаційні анкети, висновки тощо) про проведення атестацій, що не увійшли до особових справ	Інформація		Обмежений
162	Журнал обліку осіб, направлених у відрядження	Інформація		Обмежений
163	Реєстраційний журнал вхідних (заяв, доповідних і поясню-вальних записок тощо) документів	Інформація		Обмежений
164	Реєстраційний журнал вихідних документів	Інформація		Обмежений
165	Книга обліку видачі довідок про стаж, місце роботи	Інформація		Обмежений
166	Журнал реєстрації листків непрацездатності	Інформація		Обмежений
167	Журнал реєстрації посвідчень і перепусток	Інформація		Обмежений
168	Документи (доповідні записки, акти, листи) про порушення правил внутрішнього трудового розпорядку	Інформація		Обмежений
169	Документи (заявки, відомості, листи) про потребу виконкому районної в місті ради у працівниках	Інформація		Обмежений
170	Документи (листки з обліку кадрів, заяви, подання, доповідні та пояснювальні записки, довідки, обхідні листки) до розпоряджень голови районної в місті ради, що не увійшли до складу особових справ	Інформація		Обмежений
171	Документи (плани, довідки, картки, списки, графіки, листи) про періодичні медичні огляди	Інформація		Обмежений
172	Копії довідок, виданих працівникам про стаж і місце роботи, заробітну плату тощо	Інформація		Обмежений
173	Документи (листки з обліку кадрів, анкети, автобіографії, заяви) осіб, не прийнятих на роботу	Інформація		Обмежений
174	Електронний документообіг	Інформація	Структурні підрозділи та галузеві спеціалісти	Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
175	Електронна пошта	Інформація	Загальний відділ, управління праці та соціального захисту населення	Обмежений
176	Службова інформація на персональних комп’ютерах	Інформація	Структурні підрозділи та галузеві спеціалісти	Обмежений
177	Службова інформація на мобільних носіях інформації	Інформація	Структурні підрозділи та галузеві спеціалісти	Обмежений
Приміщення				
178	Робочі приміщення (кабінети)	Приміщення	Структурні підрозділи та галузеві спеціалісти	Обмежений
179	Серверне приміщення	Приміщення	Управління праці та соціального захисту населення	Обмежений
180	Відокремлені архівні приміщення	Приміщення	Структурні підрозділи та галузеві спеціалісти	Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
181	Архівні приміщення у відділі	Приміщення	Структурні підрозділи та галузеві спеціалісти	Обмежений
Обладнання				
182	Робочі станції	Обладнання	Структурні підрозділи та галузеві спеціалісти	Обмежений
183	Периферійне обладнання (принтери, сканери тощо)	Обладнання	Структурні підрозділи та галузеві спеціалісти	Обмежений
184	Телефонний та факсимільний зв’язок	Обладнання	Структурні підрозділи та галузеві спеціалісти	Обмежений
185	Комутаційне та мережеве обладнання	Обладнання	Структурні підрозділи та галузеві спеціалісти	Обмежений
186	Локальна мережа	Обладнання	Структурні підрозділи та галузеві спеціалісти	Обмежений
187	Мобільні носії інформації	Обладнання	Структурні підрозділи та	Обмежений

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Рівні доступу до активу*
			галузеві спеціалісти	
188	Сервер (АСОПД)	Обладнання	Управління праці та соціального захисту населення	Обмежений
189	Сервер (субсидії)	Обладнання	Управління праці та соціального захисту населення	Обмежений
190	Сервер (ЄДАРП)	Обладнання	Управління праці та соціального захисту населення	Обмежений

Керуючий справами виконкому ***Олександр Гижко***

Додаток 9
до розпорядження голови
районної в місті ради
від 24.11.2021 № 345-р

Реєстр
ризиків виконкому Довгинцівської районної в місті ради

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
Імідж та репутація				
1	Імідж та репутація	Імідж та репутація	Структурні підрозділи та галузеві спеціалісти	Розголошення, порушення цілісності та обмеження доступу до конфіденційної інформації. Порушення вимог ІБ через невчасну актуалізація таких вимог.
Персонал				
2	Голова районної в місті ради	Персонал	Голова районної в місті ради	Часткова або значна втрата через розголошення конфіденційної інформації під час роботи та після звільнення. Впливання на процеси інформаційної безпеки через відсутність відповідних даних щодо ефективного керування процесами ІБ. Призупинення розвитку діяльності через не контрольовану постійну або тимчасову відсутність керівника.
3	Заступник голови районної в місті ради, заступники голови районної в місті ради з питань діяльності виконавчих органів,	Персонал	Заступник голови районної в місті ради, заступники голови районної в місті ради з питань діяльності	Часткова або значна втрата через розголошення конфіденційної інформації під час роботи та після звільнення.

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
	керуючий справами виконкому районної в місті ради		виконавчих органів, керуючий справами виконкому районної в місті ради	Впливання на процеси інформаційної безпеки через відсутність відповідних даних щодо ефективного керування процесами ІБ.
4	Персонал	Персонал	Структурні підрозділи та галузеві спеціалісти	Часткова або значна втрата через розголошення конфіденційної інформації під час роботи та після звільнення. Розголошення, втрата або обмеження доступу до інформації через невчасне попередження персоналу про загрози інформаційної безпеки. Втрата або витік конфіденційної інформації через дії третіх осіб. Витік конфіденційної інформації через наявність доступу персоналу до електронної інформації. Розголошення інформації через невірне інформування про рівень її конфіденційності, невідповідне маркування інформації.
Інформація				
5	Ордера на виконання земляних робіт	Інформація	Відділ з питань благоустрою, транспорту та житла	Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Втрата інформації в разі виникнення пожежі або інших надзвичайних ситуацій. Псування документів через вплив на них факторів навколишнього середовища.

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
				Порушення конфіденційності або втрата документів через доступність третіх осіб до приміщення кабінету.
6	Протоколи засідань громадської комісії з житлових питань	Інформація		Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Втрата інформації в разі виникнення пожежі чи інших надзвичайних ситуацій. Псування документів через вплив на них факторів навколишнього середовища.
7	Журнал обліку видачі ордерів на житлову площу (виданих виконкомом районної в місті ради, підприємствами та виконкомами інших районів міста Кривого Рогу)	Інформація		
8	Журнал обліку видачі ордерів на службові жилі приміщення	Інформація		
9	Облікові справи осіб, які перебувають на квартирному обліку для поліпшення житлових умов	Інформація		
10	Книга обліку осіб, які перебувають на квартирному обліку для поліпшення житлових умов при виконкомі районної в місті ради	Інформація		
11	Документація з цивільного захисту населення і території району від надзвичайних ситуацій техногенного характеру	Інформація	Відділ з питань мобілізаційної роботи, надзвичайних ситуацій та цивільного захисту населення	Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Втрата інформації в разі виникнення пожежі чи інших надзвичайних ситуацій. Псування документів через вплив на них факторів навколишнього середовища.
12	Документація з мобілізації та мобілізаційної роботи, взаємодії та координаційної діяльності	Інформація	Відділ з питань мобілізаційної роботи, надзвичайних	

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
	правоохоронних органів та громадських формувань з охорони громадського порядку		ситуацій та цивільного захисту населення	
13	Автоматична система «КАІ-Документообіг. Електронний документообіг»	Інформація	Загальний відділ	Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Неможливість здійснювати діяльність внаслідок відсутності підключення до локальної чи зовнішньої мережі. Витік інформації в наслідок не врегульованого отримання даних на переносних носіях інформації. Втрата інформації внаслідок ураження комп'ютерними вірусами або реалізації хакерської атаки. Втрата інформації внаслідок виходу зі строю апаратної частини робочої станції. Втрата інформації через доступність до системних файлів ПЗ. Тривале переривання діяльності в наслідок не узгоджених строків з підрядними організаціями або відсутності узгоджених підрядників щодо встановлення, оновлення чи відновлення роботи ПЗ.
14	Автоматична система «КАІ-Документообіг. Звернення громадян»	Інформація		
15	Номенклатура справ	Інформація		Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними.
16	Листування з обласною державною адміністрацією з питань основної діяльності	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
17	Листування з обласною радою з питань основної діяльності	Інформація		Втрата інформації в разі виникнення пожежі чи інших надзвичайних ситуацій. Псування документів через вплив на них факторів навколишнього середовища. Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Втрата інформації в разі виникнення пожежі чи інших надзвичайних ситуацій. Псування документів через вплив на них факторів навколишнього середовища.
18	Листування з міським головою, його заступниками, керуючою справами, структурними підрозділами виконкому міськради з основних питань діяльності	Інформація		
19	Протоколи засідань виконкому районної в місті ради та документи до них	Інформація		
20	Протоколи сесій районної в місті ради та документи до них	Інформація		
21	Розпорядження голови районної в місті ради	Інформація		
22	Журнал обліку бланків суворої звітності	Інформація		
23	Листування з організаціями, установами, підприємствами з питань роботи промислових підприємств, надання послуг, випуску товарів народного вжитку	Інформація		
24	Листування з організаціями з питань будівництва, благоустрою та утримання житлового та комунального фонду	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
25	Листування з питань санітарного стану та екології на підприємствах району	Інформація		
26	Листування з питань роботи радіо, телефонної мережі, електрифікації, транспорту, ремонту і експлуатації	Інформація		
27	Листування з організаціями з питань діяльності релігійних громад	Інформація		
28	Листування з питань роботи державної і комерційної торгівлі, громадського харчування та побутового обслуговування, про експлуатацію і надання приміщень організації, здавання й приймання будівель в оренду	Інформація		
29	Листування з питань охорони здоров’я та соціального захисту населення	Інформація		
30	Листування з питань роботи закладів освіти, дошкільних закладів, організації літнього відпочинку дітей	Інформація		
31	Листування з організаціями з питань діяльності закладів культури та спорту	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
32	Листування з правоохоронними органами, територіальними центрами комплектування та соціальної підтримки, самостійними державними пожежними частинами з питань основної діяльності	Інформація		
33	Листування з питань роботи добровільних громадських організацій та партій	Інформація		
34	Листування з питань фінансової, індивідуально-трудової та кооперативної діяльності	Інформація		
35	Листування з банками, друкарнями, редакціями, організаціями з адміністративно-господарських питань	Інформація		
36	Звернення (пропозиції, заяви і скарги) громадян з питань особистого характеру та листування про їх перевірку	Інформація		
37	Список дітей пільгових категорій, рекомендованих для оздоровлення і відпочинку	Інформація	Відділ справах сім'ї, молоді та спорту	Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Втрата інформації в разі виникнення пожежі або інших надзвичайних ситуацій. Псування документів через вплив на них факторів навколишнього середовища.
38	Банк даних багатодітних сімей по району м.Кривого Рогу	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
39	Список депутатів	Інформація	Організаційний відділ	Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Втрата інформації в разі виникнення пожежі або інших надзвичайних ситуацій. Псування документів через вплив на них факторів навколишнього середовища. Порушення конфіденційності або втрата документів через доступність третіх осіб до приміщення кабінету.
40	Структура органів самоорганізації населення	Інформація		
41	Дислокація органів самоорганізації населення	Інформація		
42	Плани роботи районної в місті ради та її виконавчого комітету на місяць, квартал, півріччя	Інформація		
43	АІС «Місцеві бюджети рівня міста, району»	Інформація	Фінансовий відділ	Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Неможливість здійснювати діяльність внаслідок відсутності підключення до локальної чи зовнішньої мережі. Витік інформації в наслідок не врегульованого отримання даних на переносних носіях інформації Втрата інформації внаслідок ураження комп'ютерними вірусами або реалізації хакерської атаки Втрата інформації внаслідок виходу зі строю апаратної частини робочої станції. Втрата інформації через доступність до системних файлів ПЗ. Тривале переривання діяльності в наслідок не узгоджених строків з підрядними організаціями
44	АІС «Соціальні виплати»	Інформація		
45	База даних Єдиної інформаційно-аналітичної системи «Діти» (ЄІАС «Діти»)	Інформація	Служба у справах дітей	

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
				або відсутності узгоджених підрядників щодо встановлення, оновлення чи відновлення роботи ПЗ.
46	Списки релігійних громад району, політичних партій району, громадських організацій району та копії їх установчих документів	Інформація	Відділ з питань внутрішньої політики, взаємодії із засобами масової інформації та промоцій	Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Втрата інформації в разі виникнення пожежі або інших надзвичайних ситуацій. Псування документів через вплив на них факторів навколишнього середовища.
47	Паспорт району	Інформація		Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Втрата інформації в разі виникнення пожежі або інших надзвичайних ситуацій. Псування документів через вплив на них факторів навколишнього середовища. Порушення конфіденційності або втрата документів через доступність третіх осіб до приміщення кабінету.
48	Офіційний вебсайт виконкому районної в місті ради в мережі Інтернет (http://www.dlgr.gov.ua)	Інформація	Відділ інформаційних технологій	Втрата доступу до сайту та порушення цілісності інформації внаслідок хакерської атаки. Обмеження доступу до інформації через некероване втручання до механізмів адміністрування сайту.

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
				Тривале переривання доступу в наслідок неузгоджених строків з підрядними організаціям щодо відновлення роботи сайту.
49	Списки дітей і підлітків шкільного віку на навчальний рік	Інформація	Відділ освіти	Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Втрата інформації в разі виникнення пожежі або інших надзвичайних ситуацій. Псування документів через вплив на них факторів навколишнього середовища. Порушення конфіденційності або втрата документів через доступність третіх осіб до приміщення кабінету.
50	Списки дітей з інвалідністю, які навчаються в загальноосвітніх закладах	Інформація		
51	Журнал протоколів засідань адміністративної комісії	Інформація	Секретар адміністративної комісії	Вразливості користування та зберігання паперових документів, тобто влив на них факторів навколишнього середовища, втрата документів через пожежу або інших надзвичайних ситуацій. Також присутні можливості такі документи дублювати та переміщати поза зону користування, з чим пов’язана втрата конфіденційності документів.
52	Програма в системі ЕМСКП від НОВА-КОМ	Інформація	Відділ бухгалтерського обліку	Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Неможливість здійснювати діяльність внаслідок відсутності підключення до локальної чи зовнішньої мережі.
53	База даних M.E.DOC	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
				Витік інформації в наслідок не врегульованого отримання даних на переносних носіях інформації Втрата інформації внаслідок ураження комп'ютерними вірусами або реалізації хакерської атаки Втрата інформації внаслідок виходу зі строю апаратної частини робочої станції. Тривале переривання діяльності в наслідок не узгоджених строків з підрядними організаціями або відсутності узгоджених підрядників щодо встановлення, оновлення чи відновлення роботи ПЗ.
54	Клієнтське програмне забезпечення «ПриватБанк»	Інформація		Компрометація дій у клієнт-банку через наявність однакових паролів у всіх співробітників Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Неможливість здійснювати діяльність внаслідок відсутності підключення до зовнішньої мережі. Втрата інформації внаслідок ураження комп'ютерними вірусами або реалізації хакерської атаки. Втрата інформації внаслідок виходу зі строю апаратної частини робочої станції. Тривале переривання діяльності в наслідок не узгоджених строків з підрядними організаціями

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
				або відсутності узгоджених підрядників щодо встановлення, оновлення чи відновлення роботи ПЗ.
55	База даних прикладного програмного засобу «Фіндокументи» МережаМ (формування на електронних та паперових носіях зведених кошторисів, розподілів, зобов'язань і платіжних доручень по державному та місцевому бюджетах)	Інформація		Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Неможливість здійснювати діяльність внаслідок відсутності підключення до локальної чи зовнішньої мережі. Витік інформації в наслідок не врегульованого отримання даних на переносних носіях інформації. Втрата інформації внаслідок ураження комп'ютерними вірусами або реалізації хакерської атаки. Втрата інформації внаслідок виходу зі строю апаратної частини робочої станції. Втрата інформації через доступність до системних файлів ПЗ. Тривале переривання діяльності в наслідок не узгоджених строків з підрядними організаціями або відсутності узгоджених підрядників щодо встановлення, оновлення чи відновлення роботи ПЗ.
56	Документація службових розслідувань стосовно осіб, уповноважених на виконання функцій	Інформація	Головний спеціаліст з питань взаємодії з правоохоронними	Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними.

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
	держави або місцевого самоврядування		органами та запобігання корупції	Втрата інформації в разі виникнення пожежі або інших надзвичайних ситуацій. Псування документів через вплив на них факторів навколишнього середовища.
57	Документація спеціальних перевірок відомостей щодо осіб, які претендують на зайняття посад, пов'язаних із виконанням функцій держави або місцевого самоврядування	Інформація		Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Втрата інформації в разі виникнення пожежі або інших надзвичайних ситуацій. Псування документів через вплив на них факторів навколишнього середовища.
58	Документація конкурсних торгів	Інформація	Відділ економіки та промисловості	Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Втрата інформації в разі виникнення пожежі або інших надзвичайних ситуацій. Псування документів через вплив на них факторів навколишнього середовища. Порушення конфіденційності або втрата документів через доступність третіх осіб до приміщення кабінету.
59	Документи (програми, анкети, схеми, звіти, висновки тощо) щодо запровадження системи управління якістю	Інформація		
60	База даних призначення і надання населенню компенсації додаткових витрат на оплату комунальних послуг в умовах підвищення цін і тарифів на послуги	Інформація	Управління праці та соціального захисту населення	Втрата конфіденційності, цілісності та доступності через відсутність резервного копіювання, через дію вірусів або неконтрольованого копіювання та доступу до даної інформації.

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
61	База даних системи автоматизованої діяльності служб житлових субсидій (НАШ ДІМ)	Інформація		Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Неможливість здійснювати діяльність внаслідок відсутності підключення до локальної чи зовнішньої мережі. Витік інформації в наслідок не врегульованого отримання даних на переносних носіях інформації Втрата інформації внаслідок ураження комп'ютерними вірусами або реалізації хакерської атаки Втрата інформації внаслідок виходу зі строю апаратної частини робочої станції. Втрата інформації через доступність до системних файлів ПЗ. Тривале переривання діяльності в наслідок не узгоджених строків з підрядними організаціями або відсутності узгоджених підрядників щодо встановлення, оновлення чи відновлення роботи ПЗ.
62	База даних автоматизованої системи обробки пенсійної документації (АСОПД/КОМ-ТЕХ) та Asopdsoc	Інформація		
63	База даних програмного забезпечення M.E.DOC	Інформація		
64	База даних Єдиного державного автоматизованого реєстру осіб, які мають право на пільги (ЄДАРП)	Інформація		
65	База даних Центрального банку даних з проблем інвалідності	Інформація		
66	Інформаційно-аналітична система обліку інвалідів та дітей-інвалідів (Центральний банк даних з проблем інвалідності)	Інформація		
67	Методичні рекомендації, правила, положення, надіслані департаментом соціального захисту населення Дніпропетровської облдержадміністрації	Інформація		
68	Накази начальника управління з основної діяльності	Інформація		Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними.

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
				Втрата інформації в разі виникнення пожежі або інших надзвичайних ситуацій. Псування документів через вплив на них факторів навколишнього середовища. Порушення конфіденційності або втрата документів через доступність третіх осіб до приміщення кабінету.
69	Посадові інструкції	Інформація		Розповсюдження чи обмеження доступу до інформації внаслідок одноосібного володіння даними. Втрата інформації в разі виникнення пожежі або інших надзвичайних ситуацій. Псування документів через вплив на них факторів навколишнього середовища.
70	Журнал реєстрації письмових звернень громадян з питань особистого характеру	Інформація		
71	Книги реєстрації вхідної, вихідної документації, вхідних та вихідних телефонограм	Інформація		
72	Журнали, реєстрації прийому громадян з особистих питань керівниками управління	Інформація		
73	Протоколи оперативних нарад при керівнику управління	Інформація		
74	Документи (листування, доповідні записки, акти обстежень) відповідей про стан розгляду пропозицій, заяв та скарг громадян	Інформація		
75	Листування з підприємствами, установами, організаціями з	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
	питань основної діяльності (вхідна та вихідна кореспонденція)			
76	Листування з виконкомом Криворізької міської ради з основних питань діяльності управління	Інформація		
77	Журнал реєстрації наказів з основної діяльності управління	Інформація		
78	Журнал обліку зберігання печаток та штампів	Інформація		
79	Номенклатура справ управління	Інформація		
80	Звіти щодо стану призначення та виплати одержувачам державних соціальних допомог, компенсацій, субсидій: річні, квартальні, місячні	Інформація		
81	Протоколи засідань комісії виконкому районної у місті ради з вирішення питань, пов’язаних з наданням населенню пільг, субсидій на житлово-комунальні послуги та державної соціальної допомоги малозабезпеченим сім’ям	Інформація		
82	Журнал реєстрації прийому заяв та документів для	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
	призначення усіх видів соціальної допомоги			
83	Журнал обробки заяв (особових справ)	Інформація		
84	Журнал обліку справ, переданих до архіву	Інформація		
85	Журнали реєстрації заяв громадян, які постраждали внаслідок Чорнобильської катастрофи, на санаторно-курортне лікування категорій 1, 2, 3	Інформація		
86	Журнал реєстрації заяв на санаторно-курортне лікування дітей, які постраждали внаслідок Чорнобильської катастрофи	Інформація		
87	Журнал реєстрації заяв на санаторно-курортне лікування дітей, які постраждали внаслідок Чорнобильської катастрофи, з батьками	Інформація		
88	Журнал видачі путівок громадянам, які постраждали внаслідок Чорнобильської катастрофи	Інформація		
89	Звіти з питань забезпечення громадян, які постраждали внаслідок Чорнобильської катастрофи, санаторно-курортними путівками	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
90	Особові справи одержувачів державних соціальних допомог, компенсацій та субсидій	Інформація		
91	Журнал обліку заяв та заяви ветеранів війни, які бажають отримати путівки на санаторно-курортне лікування	Інформація		
92	Журнал обліку заяв та заяви осіб з інвалідністю, які бажають отримати путівки на санаторно-курортне лікування	Інформація		
93	Журнал обліку заяв та заяви осіб з інвалідністю загального захворювання, інвалідів з дитинства, які бажають отримати путівки на санаторно-курортне лікування	Інформація		
94	Журнал реєстрації заяв на забезпечення технічними та іншими засобами реабілітації	Інформація		
95	Журнал обліку заяв громадян щодо направлення їх до будинку-інтернату на постійне місце проживання	Інформація		
96	Журнал реєстрації заяв осіб з інвалідністю, законних представників дітей з інвалідністю на забезпечення автомобілями	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
	безкоштовно або на пільгових умовах			
97	Журнал обліку осіб з інвалідністю на забезпечення автомобілями безкоштовно або на пільгових умовах (у порядку загальної черги)	Інформація		
98	Книга обліку видачі путівок в санаторії	Інформація		
99	Журнал обліку надання компенсацій на бензин, ремонт та технічне обслуговування автомобілів, транспортні видатки	Інформація		
100	Особові справи осіб з інвалідністю – отримувачів компенсацій на бензин, ремонт та технічне обслуговування автомобілів	Інформація		
101	Журнал обліку виплат компенсацій по санаторно-курортному лікуванню осіб з інвалідністю та особисті заяви	Інформація		
102	Журнал реєстрації заяв і заяви інвалідів та непрацюючих малозабезпечених осіб на отримання матеріальної допомоги	Інформація		
103	Особові справи громадян, які перебувають під опікою чи піклуванням	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
104	Журнал обліку заяв громадян району на обслуговування у відділенні організації надання адресної натуральної та грошової допомоги КУ «Територіальний центр соціального обслуговування (надання соціальних послуг) у Довгинцівському районі»	Інформація		
105	Журнал реєстрації заяв громадян району на обслуговування КУ «Територіальний центр соціального обслуговування (надання соціальних послуг) у Довгинцівському районі»	Інформація		
106	Журнал реєстрації заяв для встановлення статусу згідно з законами України «Про статус ветеранів війни, гарантії їх соціального захисту» та «Про жертви нацистських переслідувань», заяви з відповідними пакетами документів	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
107	Журнал обліку видачі бланків суворої звітності (пільгові посвідчення та\або вкладки): - «інвалід війни» - «учасник війни» - член сім'ї загиблого (померлого) ветерана війни»	Інформація		
108	Журнал обліку видачі бланків суворої звітності – листів-талонів на пільговий проїзд ветеранам війни	Інформація		
109	Журнал реєстрації видачі довідок про перебування на обліку в Єдиному державному автоматизованому реєстрі осіб, які мають право на пільги	Інформація		
110	Журнал реєстрації особових справ громадян пільгової категорії	Інформація		
111	Особові справи громадян пільгової категорії	Інформація		
112	Журнал реєстрації заяв пільговиків по наданню пільг на тверде паливо готівкою	Інформація		
113	Журнал реєстрації заяв пільговиків по наданню пільг на скраплений газ готівкою	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
114	Журнал реєстрації заяв родичів померлих учасників бойових дій та інвалідів війни для отримання компенсації на поховання	Інформація		
115	Особові справи родичів померлих учасників бойових дій та інвалідів війни для отримання компенсації на поховання	Інформація		
116	Журнал реєстрації повідомлень про реєстрацію смерті громадян, наданих до відома органами МВС	Інформація		
117	Повідомлення про реєстрацію смерті громадян району міста Кривого Рогу	Інформація		
118	Книга обліку черги на виконання безоплатних капітальних ремонтів житлових будинків і квартир, що перебувають у власності осіб, яким надаються пільги згідно із законами України «Про статус ветеранів війни, гарантії їх соціального захисту», «Про жертви нацистських переслідувань» та «Про основні засади соціального захисту ветеранів праці та інших	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
	гро-мадян похилого віку в Україні»			
119	Книга обліку житлових будинків і квартир, що перебувають у власності осіб, яким надаються пільги згідно із законами України «Про статус ветеранів війни, гарантії їх соціального захисту», «Про жертви нацистських переслідувань» та «Про основні засади соціального захисту ветеранів праці та інших громадян похилого віку в Україні», в яких проведено такий ремонт	Інформація		
120	Особові рахунки одержувачів соціальних допомог	Інформація		
121	Журнал обліку прийому інформації електронною поштою	Інформація		
122	Журнал реєстрації довідок про отримання (не отримання) допомог та компенсацій	Інформація		
123	Журнал реєстрації виплатних документів	Інформація		
124	Звіти про нарахування на загальнообов'язкове державне пенсійне страхування за деякі категорії застрахованих осіб	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
125	Рішення, протоколи засідань комісії виконкому районної в місті ради з вирішення питань, пов’язаних з наданням матеріальної допомоги мешканцям району у зв'язку з похованням деяких категорій осіб та скрутним матеріальним становищем	Інформація		
126	Журнал реєстрації особистих звернень громадян до соціального інспектора	Інформація		
127	Журнал реєстрації виявлених порушень та стану відшкодування надміру нарахованих коштів	Інформація		
128	Журнал реєстрації запитів та відповідей до установ, організацій та підприємств для перевірок довідок про доходи	Інформація		
129	Журнал реєстрації перевірок цільового використання коштів допомоги при народженні дитини	Інформація		
130	Журнал реєстрації актів обстеження матеріально-побутових умов проживання сім’ї на матеріальну допомогу	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
131	Журнал реєстрації особових справ одержувачів усіх видів державної соціальної допомоги які перевіряються щодо правильності призначення допомоги	Інформація		
132	Журнал реєстрації актів обстеження матеріально-побутових умов проживання сім'ї та особових справ одержувачів субсидій з зазначенням тих, які розглядаються комісійно	Інформація		
133	Журнал реєстрації судових справ та особові справи отримувачів допомог, що наявні в провадженні районного суду	Інформація		
134	Реєстр колективних договорів району м. Кривого Рогу	Інформація		
135	Документи (довідки, доповідні записки, звіти, листи) про виконання пропозицій за результатами обстежень, перевірок, запитів відділу праці та соціально-трудових відносин	Інформація		
136	Свідоцтва про Державну реєстрацію юридичної особи.	Інформація		
137	Виписка з Єдиного реєстру юридичних осіб та фізичних осіб-підприємців	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
138	База даних інформаційної системи «Картка»	Інформація	Відділ з питань кадрової роботи	Непрацездатність програмного забезпечення внаслідок того, що не чітко зазначені вимоги з підтримки програмного забезпечення Втрата інформації через відсутність резервних копій бази даних. Втрата бази даних співробітників в наслідок зберігання її на персональному комп'ютері. Втрата інформації через доступність до системних файлів ПЗ.
139	Розпорядження голови районної в місті ради з кадрових питань (особового складу)	Інформація		
140	Розпорядження голови районної в місті ради про короткострокові відрядження	Інформація		
141	Розпорядження голови районної в місті ради про надання щорічних оплачуваних відпусток та відпусток у зв'язку з навчанням	Інформація		
142	Положення про структурні підрозділи виконкому районної в місті ради, та зміни до них (копії)	Інформація		
143	Особові справи працівників виконкому районної в місті ради	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
144	Особові картки працівників (у тому числі тимчасових та працюючих за сумісництвом)	Інформація		
145	Протоколи засідань конкурсних комісій із заміщення вакантних посад, обрання на посаду	Інформація		
146	Трудові книжки працівників виконкому районної в місті ради	Інформація		
147	Перелік розпоряджень голови районної в місті ради з кадрових питань (особового складу)	Інформація		
148	Перелік розпоряджень голови районної в місті ради про короткострокові відрядження	Інформація		
149	Перелік розпоряджень голови районної в місті ради про надання щорічних оплачуваних відпусток та відпусток у зв'язку з навчанням	Інформація		
150	Журнал обліку руху особових справ посадових осіб виконкому районної в місті ради	Інформація		
151	Журнал приймання працівників (у тому числі тимчасових)	Інформація		
152	Журнал переміщення працівників (у тому числі тимчасових)	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
153	Журнал звільнення працівників (у тому числі тимчасових)	Інформація		
154	Журнал обліку видачі трудових книжок і вкладок до них	Інформація		
155	Статистичні (річні) звіти з кадрових питань	Інформація		
156	Документи (нормативи чисельності, типові структури апарату, аналітичні таблиці, розрахунки, доповіді, довідки) про вдосконалення структури виконкому районної в місті ради	Інформація		
157	Документи (протоколи, подання, анкети, акти тощо) про встановлення персональних окладів, надбавок, доплат	Інформація		
158	Посадові та робочі інструкції працівників виконкому районної в місті ради	Інформація		
159	Документи (акти, постанови, рішення, довідки, доповідні та пояснювальні записки, висновки, листи) службових розслідувань	Інформація		
160	Документи (звіти, довідки, висновки, доповідні записки) про переведення працівників на	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
	скорочений робочий день або неповний робочий тиждень			
161	Документи (плани, звіти, копії наказів, листи) про стажування	Інформація		
162	Списки кандидатів на висування за посадою (резерв)	Інформація		
163	Протоколи засідань, рішення атестаційної комісії	Інформація		
164	Документи (характеристики, атестаційні анкети, висновки тощо) про проведення атестацій, що не увійшли до особових справ	Інформація		
165	Журнал обліку осіб, направлених у відрядження	Інформація		
166	Реєстраційний журнал вхідних (заяв, доповідних і пояснювальних записок тощо) документів	Інформація		
167	Реєстраційний журнал вихідних документів	Інформація		
168	Книга обліку видачі довідок про стаж, місце роботи	Інформація		
169	Журнал реєстрації листків непрацездатності	Інформація		
170	Журнал реєстрації посвідчень і перепусток	Інформація		

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
171	Документи (доповідні записки, акти, листи) про порушення правил внутрішнього трудового розпорядку	Інформація		
172	Документи (заявки, відомості, листи) про потребу виконкому районної в місті ради у працівниках	Інформація		
173	Документи (листки з обліку кадрів, заяви, подання, доповідні та пояснювальні записки, довідки, обхідні листки) до розпоряджень голови районної в місті ради, що не увійшли до складу особових справ	Інформація		
174	Документи (плани, довідки, картки, списки, графіки, листи) про періодичні медичні огляди	Інформація		
175	Копії довідок, виданих працівникам про стаж і місце роботи, заробітну плату тощо	Інформація		
176	Документи (листки з обліку кадрів, анкети, автобіографії, заяви) осіб, не прийнятих на роботу	Інформація		
177	Електронний документообіг	Інформація	Структурні підрозділи та галузеві спеціалісти	Неконтрольоване розповсюдження інформації співробітниками.

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
				Втрата інформації через некомпетентну роботу в програмному забезпеченні та відсутності усвідомлення уразливостей програмного забезпечення.
178	Електронна пошта	Інформація	Загальний відділ, управління праці та соціального захисту населення	Обмеження доступу до сховища електронної пошти через втрату авторизаційних даних (логін, пароль тощо). Неконтрольоване розповсюдження інформації співробітниками відділу. Втрата інформації через некомпетентну роботу в програмному забезпеченні. Тривале переривання діяльності внаслідок не узгоджених строків з підрядними організаціями або відсутності узгоджених підрядників щодо встановлення, оновлення чи відновлення роботи ПЗ.
179	Службова інформація на персональних комп'ютерах	Інформація	Структурні підрозділи та галузеві спеціалісти	Витік інформації через недосконалий контроль доступу до документів.
180	Службова інформація на мобільних носіях інформації	Інформація	Структурні підрозділи та галузеві спеціалісти	Розповсюдження та втрата інформації через відсутність формалізованої політики використання мобільних носіїв інформації та неконтрольованого доступу до інформації працівниками
Приміщення				
181	Робочі приміщення (кабінети)	Приміщення	Структурні підрозділи та галузеві спеціалісти	Розповсюдження чи втрата інформації з причини наявності доступу відвідувачів до кабінетів.

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
182	Серверне приміщення	Приміщення	Управління праці та соціального захисту населення	Розповсюдження чи втрата інформації з причини одноосібного доступу до приміщення чи інформації.
183	Відокремлені архівні приміщення	Приміщення	Структурні підрозділи та галузеві спеціалісти	Втрата інформації в документах через не дотримання кліматичних умов та температурного режиму зберігання документів. Викрадення інформації через відсутню охорону в денний час. Потрапляння вогню до сховищ із зовні через відкриті вікна у сховищах
184	Архівні приміщення у відділі	Приміщення	Структурні підрозділи та галузеві спеціалісти	Втрата інформації в документах через не дотримання кліматичних умов та температурного режиму зберігання документів. Знаходження сторонніх осіб в службових приміщеннях. Втрата документів у разі виникнення пожежі.
Обладнання				
185	Робочі станції	Обладнання	Структурні підрозділи та галузеві спеціалісти	Втрата інформації внаслідок ураження комп’ютерними вірусами або реалізації хакерської атаки. Вихід зі строю комп’ютерів внаслідок тривалого їх використання. Сповільнення діяльності або порушення безпеки через користування обладнанням, специфікації яких не відповідають потребам, зокрема до забезпечення відповідного захисту. Втрата інформації під час переміщення або ремонту, налагодження обладнання.

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
				Припинення роботи обладнання через відключення живлення та внаслідок аварій засобів життєзабезпечення. Вихід зі строю обладнання внаслідок не дотримання кліматичних умов та температурного режиму. Ураження електричним струмом обладнання та обслуговуючого персоналу внаслідок відсутності заземлення обладнання. Призупинення діяльності, припинення роботи обладнання через самовільне або некомпетентне встановлення, видалення або налаштування програмних ресурсів. Обмеження доступу до інформації через втрату (несанкціоноване змінення) або піддатливі для підбору авторизаційних даних (логін, пароль тощо). Тривале переривання діяльності в наслідок не узгоджених строків з підрядними організаціями або відсутності узгоджених підрядників щодо встановленні, оновлення чи відновлення роботи обладнання та ПЗ.
186	Периферійне обладнання (принтери, сканери тощо)	Обладнання	Структурні підрозділи та галузеві спеціалісти	Неконтрольоване розповсюдження інформації через відсутність контролю використання обладнання. Тривале переривання діяльності в наслідок не узгоджених строків з підрядними організаціями або відсутності узгоджених підрядників щодо

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
				встановленні, оновлення чи відновлення роботи обладнання.
187	Телефонний та факсимільний зв'язок	Обладнання	Структурні підрозділи та галузеві спеціалісти	Прослуховування телефонних розмов внаслідок не захищеності каналів. Пошкодження кабелю внаслідок виконання ремонтних робіт. Припинення роботи обладнання через відключення живлення та внаслідок аварій засобів життєзабезпечення. Несанкціоноване підключення до мережі. Тривале переривання діяльності в наслідок не узгоджених строків з підрядними організаціями або відсутності узгоджених підрядників щодо встановленні, оновлення чи відновлення роботи обладнання.
188	Комутаційне та мережеве обладнання	Обладнання	Структурні підрозділи та галузеві спеціалісти	Припинення роботи обладнання через відключення живлення та внаслідок аварій засобів життєзабезпечення Вихід зі строю обладнання в наслідок природних стихійних явищ Вихід зі строю обладнання внаслідок не дотримання кліматичних умов та температурного режиму Ураження електричним струмом обладнання та обслуговуючого персоналу внаслідок відсутності заземлення обладнання.

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
				Припинення роботи обладнання через відключення живлення та інших порушень, внаслідок аварій засобів життєзабезпечення. Несанкціоноване підключення до мережі. Тривале переривання діяльності в наслідок не узгоджених строків з підрядними організаціями або відсутності узгоджених підрядників щодо встановленні, оновлення чи відновлення роботи обладнання.
189	Локальна мережа	Обладнання	Структурні підрозділи та галузеві спеціалісти	Пошкодження кабелю внаслідок виконання ремонтних робіт. Тривале переривання діяльності в наслідок не узгоджених строків з підрядними організаціями або відсутності узгоджених підрядників щодо встановленні, оновлення чи відновлення роботи обладнання.
190	Мобільні носії інформації	Обладнання	Структурні підрозділи та галузеві спеціалісти	Втрата інформації через відсутність вимог до технічної придатності носіїв інформації.
191	Сервер (АСОПД)	Обладнання	Управління праці та соціального захисту населення	Втрата працездатності внаслідок постійного вмикання та вимикання сервера. Ураження електричним струмом обладнання та обслуговуючого персоналу внаслідок відсутності заземлення. Тривале переривання діяльності в наслідок не узгоджених строків з підрядними організаціями або відсутності узгоджених підрядників щодо встановленні, оновлення чи відновлення роботи обладнання.

№ з/п	*Активи*	*Клас активу*	*Розпорядник активу*	*Ризики*
192	Сервер (субсидія)	Обладнання	Управління праці та соціального захисту населення	Втрата працездатності внаслідок постійного вмикання та вимикання сервера. Ураження електричним струмом обладнання та обслуговуючого персоналу внаслідок відсутності заземлення. Тривале переривання діяльності в наслідок не узгоджених строків з підрядними організаціями або відсутності узгоджених підрядників щодо встановленні, оновлення чи відновлення роботи обладнання.
193	Сервер (ЄДАРП)	Обладнання	Управління праці та соціального захисту населення	Втрата працездатності внаслідок постійного вмикання та вимикання сервера. Ураження електричним струмом обладнання та обслуговуючого персоналу внаслідок відсутності заземлення. Тривале переривання діяльності в наслідок не узгоджених строків з підрядними організаціями або відсутності узгоджених підрядників щодо встановленні, оновлення чи відновлення роботи обладнання.

Керуючий справами виконкому ***Олександр Гижко***

Додаток 10
до розпорядження голови
районної в місті ради
від 24.11.2021 № 345-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 несанк-

ціонованими 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 кож-ного процесу:

Звіт оцінки ризиків для процесу

_____

(назва)

Загроза/ вразли-вість	***Оцінка ймовірності реалізації за-грози з ви-користанням вказаної вразливості***	***Оцінка впливу реалізації загрози на цілісність***	***Оцінка впливу реалізації загрози на конфі-денційність***	***Оцінка впливу реалізації загрози на доступність***	***Оцінка впливу реалізації загрози на спосте-режність***	***Рівень ризику за окремою парою загроза/ вразливість***
Загальний ризик процесу						

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 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

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 зупинки 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 ***Олександр Гижко***

Додаток 11
до розпорядження голови
районної в місті ради
від 24.11.2021 № 345-р

Положення
про придбання, розробку та обслуговування інформаційних систем

Зміст

1. Загальні положення

Метою даного Положення є забезпечення впевненості в тому, що безпека є невід'ємною властивістю інформаційних систем, які впроваджують, і забезпечити виконання вимог щодо безпеки під час їх розроблення та експлуатації.

Положення розповсюджується на всі структурні підрозділи виконкому.

Відповідальність за контролювання процесів придбання, розробки та обслуговування інформаційних систем, а також за контролювання дотримання

вимогам даного Положення несе керуючий справами виконкому Довгинцівської районної в місті ради.

Розподіл відповідальності за виконання кожним із процесів придбання, розробки та обслуговування інформаційних систем визначається посадовими інструкціями та розпорядженнями голови районної в місті ради.

При використанні нормативних документи, посилання на які є в даному положенні, необхідно застосовувати актуальні редакції цих документів.

2. Терміни та визначення

В даному положенні використовуються терміни та визначення понять згідно ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги», а також такі:

Валідація – процес, що дозволяє визначити, наскільки точно з позицій потенційного користувача деяка модель представляє задані сутності реального світу.

Додаток (застосунок, застосовна програма, прикладна програма) – користувацька комп'ютерна програма, що дає змогу вирішувати конкретні прикладні задачі користувача.

Інформаційна система – сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів.

Криптографічний захист інформації – вид захисту інформації, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Сальдо – різниця між надходженнями і витратами за певний проміжок часу.

Сирцевий код – будь-який набір інструкцій або оголошень, написаних комп'ютерною мовою програмування і у формі, що її може прочитати і модифікувати людина.

3. Нормативні посилання

ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги».

ISO/IEC 15408-1:2009 «Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model».

ISO/IEC 27005:2011 «Інформаційні технології. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки».

ISO/IEC 11770-1:2010 «Information technology - Security techniques - Key management - Part 1: Framework».

ISO/IEC 9796-2:2010 «Інформаційні технології. Методи забезпечення безпеки. Схеми цифрового підпису, які забезпечують відновлення повідомлень. Частина 2. Механізми на основі цілочисельної факторізації».

ISO/IEC 9796-3:2006 «Інформаційні технології. Методи забезпечення безпеки. Схеми цифрового підпису, які забезпечують відновлення повідомлень.

Частина 3. Механізми на основі дискретного логарифму.

ISO/IEC 14888-1:2008 «Information technology - Security techniques - Digital signatures with appendix -- Part 1: General».

ISO/IEC 14888-2:2008 «Information technology - Security techniques -- Digital signatures with appendix - Part 2: Integer factorization based mechanisms».

ISO/IEC 14888-3:2006 «Information technology - Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms».

4. Придбання, розробка та обслуговування інформаційних систем

4.1. Вимоги захисту інформаційних систем

Інформаційні системи включають операційні системи, інфраструктуру, додатки, готові продукти, послуги, а також додатки, розроблені користувачем. Проектування і реалізація інформаційних систем, підтримуючих організаційний процес, можуть бути вирішальними для захисту. Перед розробкою та / або реалізацією інформаційних систем повинні бути визначені та погоджені вимоги захисту.

Всі вимоги захисту повинні бути виявлені на стадії визначення вимог проекту та обґрунтовані, узгоджені і документально підтверджені як частина загального економічного обґрунтування проекту для інформаційної системи.

4.1.1. Аналіз та специфікація вимог захисту засобів управління

Формулювання вимог для нових інформаційних систем, або поліпшення існуючих інформаційних систем повинні специфікувати вимоги для засобів управління захистом.

Специфікація вимог для засобів управління повинна враховувати автоматизовані засоби управління, які потрібно впровадити в інформаційну систему, і потреби в допоміжних ручних засобах управління. Аналогічні дії повинні враховуватися при оцінці пакетів програм, розроблюваних або придбаних для додатків.

Вимоги захисту та засобів управління повинні відображати ділову цінність залучених інформаційних активів і можливий збиток для виконкому, який може відбутися в результаті збою в захисті або відсутності захисту.

Системні вимоги для захисту інформації та процесів реалізації захисту повинні бути інтегровані на ранніх стадіях проектування інформаційних систем. Засоби управління, введені на стадії проектування, значно дешевше для реалізації й обслуговування, ніж ті, які включені в ході реалізації або після реалізації.

Якщо продукти купуються, то необхідно слідувати офіційному процесу випробування і придбання. У договорах з постачальником повинні бути обумовлені певні вимоги захисту. Якщо функціональність захисту в пропонованому продукті не задовольняє встановленим вимогам, тоді ризик, що привноситься, і пов’язані з ним засоби управління мають бути переглянуті до придбання продукту. Якщо поставляються додаткові функціональні можливості і вони є причиною ризику для системи захисту, то вони повинні бути блоковані, або пропонована схема управління повинна бути переглянута, з метою визначити, чи може бути вилучено перевагу з наявної поліпшеної функціональності.

Якщо це буде визнано доречним, наприклад, з причини вартості, керівництво може захотіти використовувати незалежно оцінені та сертифіковані продукти. Додаткову інформацію про критерії оцінки для засобів захисту в області інформаційних технологій можна знайти в ISO/IEC 15408-1 або в інших стандартах з оцінки або сертифікації, за обставинами.

У технічному звіті ISO/IEC 27005 дано керівні вказівки по використанню процесів менеджменту ризиків для визначення вимог для засобів управління захистом.

4.2. Правильна обробка в додатках

Для забезпечення правильної обробки в додатках, включаючи додатки, розроблені користувачем, повинні бути спроектовані відповідні засоби управління. Ці засоби управління повинні включати валідацію вхідних даних, внутрішньої обробки і вихідних даних.

Додаткові засоби керування можуть бути необхідні для систем, які обробляють важливу, цінну або критичну інформацію, або мають вплив на таку інформацію. Такі засоби управління мають бути визначені на основі вимог захисту та оцінки ризиків.

4.2.1. Валідація вхідних даних засобу управління

Повинна здійснюватися валідація даних, які вводяться в додатки, з метою гарантування того, що ці дані є правильними і доречними.

Перевірки повинні застосовуватися до вхідних даних ділових угод, незмінних даних і таблиць. Повинні бути розглянуті наступні керівні вказівки:

1. Подвійне введення або інші перевірки вхідних даних, такі як граничні перевірки або обмеження полів конкретними діапазонами вхідних даних для того, щоб виявляти такі помилки:

- значення поза діапазону;
- невірні символи в полях даних;
- припущення або неповні дані;
- перевищення верхніх і нижніх меж обсягу даних;
- недозволені або суперечливі контрольні дані.

2. Періодичний аналіз вмісту ключових областей або файлів даних для того, щоб підтвердити їх достовірність та цілісність.

3. Контроль твердих копій вхідних документів на предмет будь-яких недозволених змін (всі зміни у вхідних документах повинні бути дозволені).

4. Процедури для реакції на помилки, виявлені валідацією.

5. Процедури для перевірки правдоподібності вхідних даних.

6. Визначення обов’язків всього персоналу, залученого в процес введення даних.

7. Створення журналу реєстрації діяльності, пов’язаної з процесом введення даних.

Можна розглянути автоматичне обстеження і валідацію вхідних даних, якщо це застосовно, для того, щоб знизити ризики помилок і запобігти стандартні атаки, включаючи переповнювання буфера і введення коду.

4.2.2. Управління внутрішньої обробкою

У додатки повинні бути вбудовані валідаційні перевірки, з метою запобігання будь-якого псування інформації внаслідок помилок обробки або умисних дій.

Проектування та реалізація програм слід забезпечувати, щоб ризики збоїв в обробці, що призводять до втрати цілісності, були мінімізовані. Конкретні області, які треба розглянути, включають наступне:

- використання функцій додавання, модифікації і видалення для того, щоб здійснювати зміни в даних;
- процедури для запобігання роботи програм в неправильному порядку або роботи після збою попередньої обробки;
- використання підходящих програм для того, щоб відновлюватися після збоїв, з метою забезпечення правильної обробки даних;
- захист від атак, що використовують перевантаження / переповнення буфера.

Повинні бути підготовлені відповідні контрольні листи, діяльність повинна бути документально підтверджена, а результати мають залишатися захищеними.

Приклади перевірок, які можна вбудувати, включають наступне:

- засоби управління з'єднаннями або пакетами для того, щоб узгодити сальдо файлів даних після поновлення угод;
- засоби управління сальдо для того, щоб перевіряти початкове сальдо по відношенню до попереднього кінцевого сальдо, а саме:
- засоби управління від виконання до виконання [run-to-run];
- підсумкові дані оновлень файлу;
- засоби управління від програми до програми [program-to-program];
- валідація вхідних даних, створюваних системою;
- перевірки на цілісність, автентичність або яку-небудь іншу характеристику захисту даних або програмного забезпечення, що завантажуються або підкачуються між центральними та віддаленими комп'ютерами;
- контрольні суми записів і файлів;
- перевірки для забезпечення того, щоб прикладні програми виконувалися в правильний час;
- перевірки для забезпечення того, щоб програми виконувалися в правильному порядку, щоб їх виконання припинялося у разі збою, і щоб подальша обробка була зупинена до тих пір, поки проблема не буде вирішена;
- створення журналу реєстрації дій, пов'язаних з обробкою.

Дані, які були введені правильно, можуть бути пошкоджені апаратними помилками, помилками обробки або внаслідок навмисних дій.

Необхідні валідаційні перевірки будуть залежати від характеру програми та ділового впливу будь-якого пошкодження даних.

4.2.3. Цілісність повідомлень

Повинні бути визначені вимоги до забезпечення автентичності та захисту цілісності повідомлень в додатках, і повинні бути визначені і реалізовані

відповідні засоби управління.

Повинна виконуватися оцінка ризиків для захисту, з метою з'ясувати, чи потрібна цілісність повідомлення, і виявити найбільш підходящі методи реалізації.

Криптографічні методи, можуть використовуватися як адекватні засоби реалізації аутентифікації повідомлень.

4.2.4. Валідація вихідних даних

Повинна здійснюватися валідація виводу даних з програми, з метою забезпечення того, щоб обробка інформації, що зберігається, була правильною і відповідною обставинам.

Валідація вихідних даних може включати в себе наступне:

- перевірки правдоподібності для того, щоб з'ясувати, чи є вихідні дані коректними;
- погодження лічильника команд для забезпечення обробки всіх даних;
- надання зчитувачу або наступній системі обробки достатньої інформації для того, щоб визначити правильність, повноту, точність і класифікацію інформації;
- процедури реагування на валідаційні випробування вихідних даних;
- визначення обов'язків всього персоналу, залученого в процес виводу даних;
- створення протоколу діяльності в процесі валідації виводу даних.

Зазвичай, системи та програми створюються на тому припущенні, що, пройшовши належну валідацію, верифікацію і випробування, документальне підтвердження, перевірку і тестуючи, вихідні дані завжди будуть правильними.

Тим не менш, це припущення не завжди вірно; тобто системи, які були випробувані, все ще можуть за деяких обставин видати вірні вихідні дані.

4.3. Криптографічні засоби управління

Метою криптографічного засобу управління є – забезпечення захисту конфіденційності, автентичності або цілісності інформації.

Повинна бути розроблена політика з використання криптографічних засобів управління. Для того щоб підтримувати використання криптографічних методів, має здійснюється розподіл ключів.

4.3.1. Політика щодо використання криптографічних засобів управління

Повинна бути розроблена і реалізована політика з використання криптографічних засобів управління для захисту інформації.

При розробці криптографічної політики має бути розглянуто наступне:

- підхід керівництва до використання криптографічних засобів управління по виконкому, включаючи загальні принципи, відповідно до яких повинна захищатися ділова інформація;
- на основі оцінки ризиків повинен бути визначений необхідний рівень захисту, з урахуванням типу, строгості і якості необхідного шифрувального алгоритму;
- використання шифрування для захисту важливої інформації, яку

переносять мобільними або змінними носіями, пристроями або через лінії зв'язку;

- підхід до розподілу ключів, включаючи методи для роботи із захистом криптографічних ключів та відновлення зашифрованої інформації в випадку втрачених, розкритих або пошкоджених ключів;

- ролі та обов'язки, наприклад, хто відповідає за наступне:

- реалізація політики;

- розподіл ключів, включаючи генерування ключів;

- стандарти, які належить прийняти для результативної реалізації у виконкомі (для якого ділового процесу яке рішення використовується);

- вплив використання зашифрованої інформації на засоби управління, які залежать від контролю вмісту (наприклад, виявлення вірусів).

При реалізації організаційної політики в області криптографії, увага повинна бути приділена нормам і державним обмеженням, які можуть ставитися до використання криптографічних методів.

Криптографічні засоби керування можуть використовуватися для досягнення інших цілей захисту, наприклад, таких:

- конфіденційність: використання шифрування інформації для захисту важливої або критичної інформації, як збереженої, так і переданої;

- цілісність / автентичність: використання цифрових підписів або кодів аутентифікації повідомлень для захисту автентичності та цілісності збереженої або переданої важливої або критичної інформації;

- використання криптографічних методів для того, щоб отримати доказ того, що відбулась подія або дія тощо.

Прийняття рішення з питання того, чи доречне криптографічне рішення, повинно розглядатися як частина більш широкого процесу оцінки ризиків і вибору засобів управління. Ця оцінка може потім бути використана для визначення того, чи доречний криптографічний засіб управління, який тип засобу управління повинен бути застосований, для якої мети і для яких ділових процесів.

Політика щодо використання криптографічних засобів управління необхідна для того, щоб витягти максимум переваг і мінімізувати ризики використання криптографічних методів, а також для того, щоб уникнути недоречного або неправильного використання. При використанні цифрових підписів, увага повинна бути приділена всім хто має відношення до справи законам, зокрема, законам, що описує умови, за яких цифровий підпис юридично обов'язковий за законом.

Треба вдатися до поради фахівця для того, щоб визначити відповідний рівень захисту і визначити відповідні специфікації, які забезпечать необхідний захист і підтримають реалізацію безпечної системи розподілу ключів.

4.3.2. Розподіл ключів

Для підтримки використання криптографічних методів необхідно застосовувати розподіл ключів.

Всі криптографічні ключі повинні бути захищені від модифікації, втрати і руйнування. Крім того, секретним і особистим ключам потрібен захист від

недозволеного розкриття. Обладнання, що використовується для того, щоб генерувати, зберігати і архівувати ключі, має бути фізично захищене.

Система розподілу ключів повинна бути заснована на узгодженому наборі стандартів, процедур і безпечних методів для наступного:

- генерування ключів для різних криптографічних систем і різних додатків;
- генерування та отримання сертифікатів відкритого ключа;
- роздача ключів призначеним користувачам, включаючи те, як ключі повинні бути активовані по отриманні;
- зберігання ключів, включаючи те, як повноважні користувачі отримують доступ до ключів;
- зміна або оновлення ключів, включаючи правила відносно того, коли ключі повинні змінюватися, і як це буде робитися;
- робота з розкритими ключами;
- анулювання ключів, включаючи те, як ключі повинні бути вилучені або дезактивовані, наприклад, якщо ключі були розкриті або якщо користувач йде з виконкому (в такому випадку ключі також повинні бути архівовані);
- відновлення ключів, які загубилися або пошкодилися, як частина менеджменту безперервності діяльності, наприклад, для відновлення зашифрованої інформації;
- архівування ключів, наприклад, для інформації, що архівується, або для інформації, резервна копія якої створюється;
- руйнування ключів;
- реєстрація і аудит дій, пов’язаних з розподілом ключів.

Для того, щоб знизити ймовірність розкриття, повинні бути визначені дати активізації та дезактивації для ключів, щоб ключі можна було використовувати тільки протягом обмеженого періоду часу. Цей період часу повинен залежати від обставин, при яких використовується криптографічний засіб управління, і від прийнятого ризику.

На додаток до захищеного розподілу секретних і приватних ключів, також повинна бути продумана аутентифікація відритих ключів. Цей процес аутентифікації може бути здійснено з використанням сертифікатів відкритого ключа, які зазвичай випускаються сертифікуючим органом, який повинен бути визнаний виконкомом з підходящими засобами управління і прийнятими процедурами для того, щоб забезпечити необхідний ступінь довіри.

Зміст угод про рівень обслуговування або договорів із зовнішніми постачальниками криптографічних послуг, наприклад, сертифікаційним органом, повинен охоплювати питання відповідальності, надійності послуг і часу реагування для надання послуг.

Розподіл криптографічних ключів є суттєвим для результативного використання криптографічних методів. ISO/IEC 11770-1 дає додаткову інформацію про розподіл ключів. Типи криптографічних методів:

- методи секретних ключів, коли дві сторони або більше спільно використовують один і той же ключ, і цей ключ використовується як для шифровки, так і для дешифрування інформації; цей ключ повинен зберігатися в секреті,

оскільки кожен, хто має доступ до ключа, має можливість декодувати всю інформацію, зашифровану з цим ключем, або ввести недозволену інформацію, використовуючи ключ;

- методи відкритих ключів, коли кожен користувач має пару ключів, відкритий ключ (який може бути відкритий кожному) і особистий ключ (який повинен триматися в секреті); методи відкритих ключів можуть використовуватися для шифрування і створення цифрових підписів.

Існує загроза підробки цифрового підпису шляхом заміни відкритого ключа користувача. Ця проблема вирішується використанням сертифіката відкритого ключа.

Криптографічні методи також можуть використовуватися для захисту криптографічних ключів. Може знадобитися передбачити процедури для обробки юридичних запитів на доступ до криптографічних ключів, наприклад, може знадобитися зробити зашифровану інформацію доступною в незашифрованому вигляді як доказ у судовій справі.

4.4. Захист системних файлів

Метою захисту системних файлів є забезпечення захисту системних файлів.

Доступ до системних файлів і вихідному тексті програми повинен керуватись, а проектування і допоміжна діяльність у галузі інформаційних технологій повинна здійснюватись захищеним способом. Необхідно дбати про те, щоб уникнути розкриття важливих даних у випробувальному середовищі.

4.4.1. Управління системним програмним забезпеченням

Повинні бути прийняті процедури для управління установкою програмного забезпечення в операційних системах.

З метою мінімізувати ризики псування для операційних систем, для управління змінами мають бути розглянуті наступні керівні вказівки:

- оновлення операційного програмного забезпечення, програм та бібліотек програм повинно виконуватися тільки підготовленими адміністраторами з відповідного дозволу керівництва;

- операційні системи повинні зберігати лише затверджені виконувані програми і не повинні зберігати програми, що знаходяться в розробці, або компілятори;

- додатки і системне програмне забезпечення повинно реалізовуватися тільки після проведення всебічних і успішних випробувань; випробування повинні включати випробування на практичність, безпеку, вплив на інші системи та зручність для користувача, і повинні виконуватися в окремих системах; повинно бути проведено оновлення всіх відповідних бібліотек вихідних програм;

- система управління конфігурацією повинна використовуватися для того, щоб зберігати контроль над всім реалізованим програмним забезпеченням, а також системною документацією;

- повинна бути прийнята стратегія відкату (відновлення попереднього стану) перш, ніж будуть реалізовуватися зміни;

- повинен вестися контрольний журнал всіх оновлень в бібліотеках системних програм;

- попередні версії прикладного програмного забезпечення повинні зберігатися на випадок надзвичайної ситуації;

- старі версії програмного забезпечення повинні зберігатися в архіві разом з усією необхідною інформацією та параметрами, процедурами, деталями конфігурації і допоміжним програмним забезпеченням стільки, скільки дані зберігаються в архіві.

Програмне забезпечення, що постачається постачальником і яке використовується в операційних системах, повинно підтримуватися на рівні, підтримуваному постачальником. З часом, програмні постачальники перестануть підтримувати більш старі версії програмного забезпечення. Виконком повинен врахувати ризики, пов'язані з розрахунком на непідтримуване програмне забезпечення.

Будь-яке рішення про перехід до нової версії повинно враховувати ділові вимоги до змін, а також захист версії, тобто введення нових функціональних можливостей в області захисту або серйозність проблем в галузі захисту, впливають на цю версію. Повинні застосовуватися латки до програмного забезпечення, якщо вони можуть допомогти усунути або зменшити слабкі місця захисту.

Фізичний або логічний доступ повинен надаватися постачальникам тільки в цілях підтримки, коли це необхідно, і з схвалення керівництва. Діяльність постачальника повинна постійно контролюватися.

Комп'ютерне програмне забезпечення може покладатися на програмне забезпечення і модулі, що поставляються ззовні, які повинні постійно контролюватися і управлятися для того, щоб уникнути недозволених змін, які можуть привнести слабкі місця в захист.

Версія операційних систем повинна змінюватися лише тоді, коли є вимога зробити так, наприклад, якщо поточна версія операційної системи більше не підтримує ділові вимоги. Зміна версій не повинна відбуватися тільки тому, що стала доступною нова версія операційної системи. Нові версії операційних систем можуть бути менш безпечними, менш стабільними і гірше розуміються, ніж поточні системи.

4.4.2. Захист випробувальних даних системи

Випробувальні дані повинні вибиратися ретельно, і повинні бути захищені і керовані.

Треба уникати використання робочих баз даних, що містять особисту інформаційну чи будь-яку іншу важливу інформацію, в цілях випробування. Якщо особиста інформація або інформація, яка важлива в іншому відношенні, використовується в цілях випробування, то всі важливі подробиці і зміст повинні бути видалені або модифіковані до невпізнання перед використанням.

Наступні керівні вказівки повинні застосовуватися для захисту робочих даних, коли ті використовуються в цілях випробування:

- процедури управління доступом, які застосовуються до робочих прикладних систем, повинні також застосовуватися до випробувальних прикладних

систем;

- повинен бути окремий дозвіл тоді, коли робоча інформація копіюється в випробувальну прикладну систему;

- робоча інформація повинна бути стерта з випробувальної прикладної системи негайно після того, як випробування буде завершено;

- копіювання та використання робочої інформації повинні бути зареєстровані для того, щоб забезпечити ведення контрольного журналу.

Системне і приймальне випробування зазвичай вимагають великих обсягів випробувальних даних, які близькі до робочих даних настільки, наскільки це можливо.

4.4.3. Управління доступом до сирцевого коду програми

Доступ до сирцевого коду програми повинен бути обмежений.

Сирцевий код програми - це код, написаний програмістами, який компілюється (і зв'язується) для того, щоб створювати модулі. Певні мови програмування не проводять формальної відмінності між сирцевим кодом і модулями, так як модулі створюються в той час, коли вони активуються.

Стандарти ISO 10007 та ISO/IEC 12207 надають додаткову інформацію про менеджмент конфігурації і процеси життєвого циклу програмного забезпечення.

Доступ до сирцевого коду програми і пов'язаних елементів (таких як проекти, специфікації, плани верифікації та плани валідації) повинен керуватися для того, щоб запобігти введенню недозволених виконуваних функцій і для того, щоб уникнути ненавмисних змін. Для сирцевого коду програми цього можна досягти шляхом керованого центрального зберігання такого коду, переважно в бібліотеках сирцевих програм. Потім повинні бути розглянуті наступні керівні вказівки для управління доступом до таких бібліотек вихідних програм, з метою знизити можливість псування комп'ютерних програм:

- де можливо, бібліотеки вихідних програм не повинні міститися в операційних системах;

- менеджмент вихідного коду програм і бібліотек вихідних програм повинен здійснюватися згідно встановлених процедур;

- допоміжний персонал не повинен мати необмежений доступ до бібліотек сирцевих програм;

- оновлення бібліотек сирцевих програм і пов'язаних елементів, а також випуск програмних джерел програмістам повинен здійснюватися тільки після того, як буде отримано відповідний дозвіл;

- роздруківки програм повинні перебувати в безпечному середовищі;

- повинен вестися контрольний журнал всіх доступів до бібліотек вихідних програм;

- супровід і копіювання бібліотек вихідних програм повинні підкорятися жорстким процедурам управління змінами.

4.5. Захист в процесах розробки та допоміжних процесах

Метою захисту в процесах розробки та допоміжних процесах є підтримування захисту прикладного системного програмного забезпечення та інформації.

Середовища проектування та допоміжні середовища повинно керуватись.

Відповідальні за прикладні системи, повинні також бути відповідальними за захист середовища проектування або допоміжного середовища. Вони повинні забезпечувати, щоб всі пропоновані зміни системи були проаналізовані для того, щоб забезпечити, що вони не піддають ризику захист або системи, або операційне середовище.

4.5.1. Процедури управління змінами

Реалізація змін повинна управлятися шляхом використання офіційних процедур управління змінами.

Офіційні процедури управління змінами повинні бути документально підтверджені і приведені у виконання для того, щоб мінімізувати порчу інформаційних систем. Введення нових систем і суттєвих змін в існуючі системи має підкорятися офіційним процесу документування, специфікації, випробування, управління якістю і керованої реалізації.

Цей процес повинен включати оцінку ризиків, аналіз впливів змін, а також специфікації необхідних засобів захисту. Цей процес також повинен забезпечувати, щоб існуючий захист і процедури керування не піддавалися ризику, щоб допоміжним програмістам був наданий доступ тільки в ті частини системи, які необхідні для їх роботи, і щоб була отримана офіційна згода та затвердження для будь-якої зміни.

Якщо тільки це практично здійснимо, то прикладні та операційні процедури управління змінами повинні бути інтегровані. Процедури зміни повинні включати в себе наступне:

- ведення запису узгоджених рівнів дозволу;
- забезпечення того, що зміни подаються повноважними користувачами;
- аналіз засобів управління і процедур забезпечення цілісності з метою гарантування того, що зміни не підданий їх ризику;
- виявлення всього програмного забезпечення, інформації, об’єктів баз даних і апаратних засобів, які вимагають поправок;
- отримання офіційного затвердження для докладних пропозицій до того як робота почнеться;
- забезпечення того, щоб повноважні користувачі прийняли зміни до реалізації;
- забезпечення того, щоб набір системної документації оновлювався по виконанню кожної зміни, і щоб стара документація архівувалася або ліквідувалася;
- підтримання управління версіями для всіх оновлень програмного забезпечення;
- ведення контрольного журналу всіх запитів на зміни;
- забезпечення того, щоб операційна документація і процедури, визначені користувачем, були змінені, як необхідно, щоб залишатися відповідними;
- забезпечення того, щоб реалізація змін відбувалася в правильний час і не заважала залученим діловим процесам.

Зміна програмного забезпечення може вплинути на операційне середовище. Хороша практика включає випробування нового програм-ного

забезпечення в середовищі, відокремленою як від виробничих середовищ, так і від середовищ розробки. Це забезпечує контроль над новим програмним забезпеченням і дає можливість додаткового захисту робочої інформації, яка використовується в випробувальних цілях. Це повинно включати в себе латки, службові пакети та інші оновлення. Автоматизовані оновлення не повинні використовуватися в критичних системах, оскільки деякі оновлення можуть викликати збій в критичних додатках.

4.5.2. Технічний аналіз додатків після змін операційної системи

Коли операційні системи змінюються, ділові критичні програми повинні аналізуватися і випробовуватися, з метою гарантування відсутності несприятливого впливу на організаційні операції або захист.

Цей процес повинен охоплювати наступне:

- аналіз процедур управління прикладними процесами і забезпечення цілісності з метою гарантування того, що вони не були піддані ризику зміни операційної системи;
- забезпечення того, що річний план підтримки та бюджет будуть охоплювати аналіз і випробування системи, що випливають із змін операційної системи;
- забезпечення того, щоб повідомлення про зміни операційної системи було надано завчасно, з метою уможливлення проведення належних випробувань та аналізу до реалізації;
- забезпечення того, щоб належні зміни були зроблені в планах забезпечення безперервності діяльності.

Спеціальна група або особа повинні бути призначені відповідальними за перевірку слабких місць і випусків латок і виправлень.

4.5.3. Обмеження на зміни в пакетах програм

Треба перешкоджати модифікаціям в пакетах програм, ці модифікації повинні бути обмежені необхідними змінами, і всі зміни повинні строго контролюватися.

На скільки можливо і практично здійснимо, пакети програм, що поставляються постачальниками, повинні використовуватися без модифікації. Якщо пакет програм необхідно модифікувати, то повинні бути розглянуті наступні пункти:

- ризики вбудованих засобів управління і процеси забезпечення цілісності, які піддаються ризику;
- чи повинна бути отримана згода постачальника;
- можливість отримання необхідних змін від постачальника у вигляді стандартних програмних оновлень;
- вплив, якщо виконком стає відповідальним за майбутній супровід програмного забезпечення в результаті змін.

Якщо зміни необхідні, то оригінальне програмне забезпечення повинно бути збережено, а зміни застосовані до чітко позначеної копії. Повинен бути реалізований процес управління оновленням програмного забезпечення для того, щоб гарантувати установку найбільш оновлених затверджених латок і оновлень

додатків для всього дозволеного програмного забезпечення. Всі зміни повинні бути повністю випробувані і документально підтверджені для того, щоб вони могли застосовуватися повторно, якщо необхідно, до майбутніх програмним оновлень. Якщо потрібно, то модифікації повинні бути випробувані і валідовані незалежним оціночним органом.

4.5.4. Витік інформації

Можливості для витоку інформації повинні бути попереджені.

Наступне повинно бути розглянуто для того, щоб обмежити ризик витоку інформації, наприклад, через використання та експлуатацію прихованих каналів:

- сканування вихідних носіїв інформації та засобів зв'язку на наявність прихованої інформації;
- маскування і модулювання поведінки систем і засобів зв'язку для того, щоб знизити ймовірність того, що третя сторона буде здатна простежити інформацію з такої поведінки;
- використання систем і програмного забезпечення, які, як вважається, мають високу цілісністю, наприклад, використовують оцінені продукти;
- регулярний постійний контроль діяльності персоналу та системи там, де це дозволено за існуючим законодавством чи нормам;
- постійний контроль використання ресурсів в комп'ютерних системах.

Приховані канали - це шляхи, які не призначені для проведення інформаційних потоків, але які можуть, тим не менш, існувати в системі або мережі. Наприклад, маніпулювання бітами в протоколах обміну пакетами може використовуватися як прихований метод сигналізації. Через їх природу, запобігання існуванню всіх можливих прихованих каналів буде важким, якщо не неможливим. Проте, експлуатація таких каналів часто здійснюється троянським кодом. Отже, прийняття заходів для захисту від троянського коду зменшує ризики експлуатації прихованих каналів. Запобігання недозволеного доступу до мережі, а також політика і процедури для того, щоб перешкоджати неправильне використання інформаційних послуг персоналом допоможуть захиститися від прихованих каналів.

4.5.5. Аутсорсінгова розробка програмного забезпечення

Аутсорсінгова розробка програмного забезпечення повинна бути під наглядом виконкому та постійно контролюватися виконкомом.

Якщо здійснюється аутсорсінг розробки програмного забезпечення, то повинні бути розглянуті наступні пункти:

- ліцензійні угоди, власність на код і права на інтелектуальну власність;
- сертифікація якості і точності виконаної роботи;
- заходи по умовному депонуванню на випадок відмови третьої сторони;
- права доступу для аудиту якості і точності зробленої роботи;
- договірні вимоги для якості та захисної функціональності коду;
- випробування перед установкою з метою виявити зловмисний і троянський код.

4.6. Менеджмент технічно слабких місць

Метою менеджменту технічно слабких місць є - зниження ризиків, які виникають при експлуатації опублікованих технічно слабких місць.

Менеджмент технічно слабких місць повинен реалізовуватися дієвим, систематичним і повторюваним способом з вимірюваннями, виконуваними для підтвердження його результативності. Ці міркування повинні включати операційні системи, а також будь-які інші програми, які використовуються.

4.6.1. Управління технічно слабкими місцями

Повинна бути отримана своєчасна інформація про технічно слабкі місця використовуваних інформаційних систем, оцінена схильність виконкому впливу таких слабких місць, і вжито належних заходів для того, щоб врахувати пов'язаний з ними ризик.

Поточний і повний опис активів - це попередня умова для результативного управління технічно слабкими місцями. Специфічна інформація, необхідна для підтримки менеджменту технічно слабких місць, включає постачальника програмного забезпечення, номера версій, поточний стан розробки (наприклад, яке програмне забезпечення в яких системах встановлено) і людина (люди) у виконкомі, відповідальні за програмне забезпечення.

Відповідну та своєчасну дію має бути розпочато у відповідь на виявлення можливих технічно слабких місць. Треба виконувати наступні настанови для того, щоб встановити результативний процес менеджменту для технічно слабких місць:

- виконком повинен визначити і встановлювати ролі та обов'язки, пов'язані з менеджментом технічно слабких місць, включаючи постійний контроль слабкого місця, оцінку ризиків слабкого місця, накладення латок, відстеження активів та будь-які необхідні обов'язки з координації;

- інформаційні ресурси, які будуть використовуватися для виявлення значущих технічно слабких місць і для підтримки поінформованості про них, повинні бути визначені для програмного забезпечення та іншої технології (заснованої на опису активів); ці інформаційні ресурси повинні оновлюватися на основі змін у опису, або коли виявляються інші нові або корисні ресурси;

- повинна бути визначена тимчасова шкала для того, щоб реагувати на повідомлення про можливі значущих технічно слабкі місця;

- як тільки можливе технічно вразливе місце буде виявлено, виконком повинен визначити пов'язані з ним ризики та дії, які потрібно вжити; така дія може включати в себе накладення латок на уразливі системи та / або застосування інших засобів управління;

- залежно від того, наскільки терміново необхідно розглянути технічно слабке місце, дію має бути виконано відповідно із засобами управління, пов'язаними з управлінням змінами або шляхом виконання процедур реагування на події в системі захисту інформації;

- якщо доступна латка, то повинні бути оцінені ризики, пов'язані з установкою латки (ризики, що накладалися вразливим місцем, повинні бути порівняні з ризиками установки латки);

- латки повинні випробовуватися та оцінюватися до того, як вони будуть встановлені, з метою забезпечити того, щоб вони були результативні, і що вони не приведуть до неприпустимих побічних ефектів; якщо ніякої латки немає в розпорядженні, то повинні бути розглянуті інші засоби управління, такі як наступні:

- відключення послуг або можливостей, пов'язаних з уразливим місцем;

- адаптація або додавання засобів управління доступом, наприклад, брандмауерів, на кордонах мереж;

- підвищений постійний контроль для того, щоб виявити або запобігти фактичній атаці;

- підвищення обізнаності про слабке місце;

- контрольний журнал повинен вестися для всіх виконуваних процедур;

- процес менеджменту технічно слабкими місцями повинен регулярно контролюватися і оцінюватися для того, щоб забезпечити його результативність та ефективність;

- системи з високим ступенем ризику повинні бути розглянуті в першу чергу.

Правильне функціонування організаційного процесу менеджменту технічно слабкими місцями критично для багатьох організацій і, отже, повинно регулярно контролюватися. Точний опис є суттєвим для забезпечення того, що можливі значущі технічно слабкі місця виявлені.

Менеджмент технічно слабкими місцями може розглядатися як підфункція управління змінами і в цій якості може використовувати в своїх інтересах процес і процедури менеджменту змін.

Постачальники часто перебувають під значним тиском щодо того, щоб випускати латки якнайскоріше. Отже, латка може не звертатися до проблеми належним чином і може мати негативні побічні ефекти. Також, в деяких випадках, видалення латки може не бути легко досяжним після того, як латка буде накладена.

Якщо необхідне випробування латок не можливе, наприклад, через витрати або нестачу ресурсів, то може бути розглянута затримка в накладенні латки, з метою оцінити пов'язаний ризик, ґрунтуючись на досвіді, про який повідомили інші користувачі.

Керуючий справами виконкому ***Олександр Гижко***

Додаток 12
до розпорядження голови
районної в місті ради
від 24.11.2021 № 345-р

Положення
про фізичну та екологічну безпеку інформації
виконкому Довгинцівської районної в місті ради

Зміст

1. Загальні положення

Ціллю даного положення є:

- запобігання несанкціонованому фізичному доступу, пошкодженню та впливу на приміщення та інформацію виконкому Довгинцівської районної в місті ради;
- запобігання втраті, пошкодженню, викраденню чи компрометації активів та припиненню діяльності виконкому Довгинцівської районної в місті ради.

При здійсненні дій пов'язаних із управлінням фізичною та екологічною безпекою керуватися даним положенням, а також настановами актуальними стандартами ISO/IEC 27001 та ISO/IEC 27002 (його національними версіями, або іншим нормативним документом, що їх замінюють).

Положення розповсюджується на всі структурні підрозділи виконкому.

Відповідальність за контролювання фізичної та екологічної безпеки, а також за контролювання дотримання вимогам даного положення несе керую-чий справами виконкому Довгинцівської районної в місті ради.

2. Терміни та визначення

В даному положенні використовуються терміни та визначення понять згідно ДСТУ ISO/IEC 27001:2015 та ISO/IEC 27002:2013.

3. Нормативні посилання

В даному положенні використовуються посилання на наступні нормативні документи:

- ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги»;
- ISO/IEC 27002:2013 «Інформаційні технології. Методи забезпечення безпеки. Звід правил по управлінню захистом інформації».

4. Безпечні зони

4.1. Фізичний периметр безпеки

Для захисту зон, які містять інформацію і засоби обробки інформації, повинні використовуватися периметри безпеки (бар'єри, такі як стіни або керовані персоналом столи реєстрації).

Периметри безпеки повинні бути чітко визначені, розміщення і потужність кожного з периметрів повинні залежати від вимог до захисту активів в межах периметра і від результатів оцінки ризику.

Периметри будівлі або місця, містять засоби обробки інформації, повинні бути фізично цілими (тобто не повинно бути ніяких проломів в периметрі або зон, де могло б легко відбутися проникнення). Зовнішні стіни місця повинні мати тверду конструкцію, а всі зовнішні двері повинні бути належним чином захищені від недозволеного доступу за допомогою механізмів управління, наприклад, решіток, сигналізації, замків тощо. Двері і вікна повинні бути замк-нені, коли знаходяться без нагляду, і повинен бути врахований зовнішній за-хист для вікон, особливо на першому поверсі.

Мають бути створені керовані персоналом столи реєстрації або інші засоби для управління фізичним доступом до місця. Доступ до місць і будівлям повинен бути обмежений тільки повноважним персоналом; там, де це може бути застосовано, повинні бути побудовані фізичні перепони, з метою запобігти недозволений фізичний доступ і екологічне забруднення навколишнього середовища.

Всі пожежостійкі двері в периметрі безпеки, повинні бути оснащені сигналізацією, постійно контролюватися і випробовуватися разом зі стінами для того, щоб встановити необхідний рівень опору відповідно до регіональних, національних та міжнародних стандартів. Вони повинні працювати безаварійно відповідно до місцевих норм пожежної безпеки.

У відповідності з національними, регіональними або міжнародними стандартами мають бути встановлені і повинні регулярно проходити випробування системи виявлення вторгнення для того, щоб охопити всі зовнішні двері і доступні вікна. Незайняті зони повинні бути під сигналізацією в будь-який час. Також має бути передбачено покриття для інших областей, наприклад, при-

міщень з встановленими в них комп'ютерами і приміщень вузлів зв'язку.

Засоби обробки інформації, керовані організацією, повинні фізично бути відділені від засобів обробки інформації, керованих третіми сторонами.

Фізичний захист може бути досягнутий шляхом створення одного або більше фізичного бар'єру навколо організаційних будівель і засобів обробки інформації. Використання декількох бар'єрів дає додатковий захист, якщо збій в роботі одного бар'єру не означає, що захист негайно піддасться ризику.

Безпечна зона може бути замкненим офісом, або декількома кімнатами, оточеними безперервним внутрішнім фізичним бар'єром безпеки. Між зонами з різними вимогами до безпеки всередині периметра безпеки можуть знадо-битися додаткові бар'єри і периметри для управління фізичним доступом.

Особлива увага до безпеки фізичного доступу має бути приділена будівлям, де розміщено кілька організацій.

4.2. Засоби управління фізичним доступом

Безпечні зони повинні бути захищені підходящими засобами управління доступом для того, щоб забезпечити, що доступ дозволений тільки повноважному персоналу.

Дата і час входу і виходу відвідувачів повинні записуватися, а всі відвідувачі повинні знаходитися під наглядом, якщо їх доступ раніше не затверджувався. Їм повинен надаватися доступ тільки для конкретних, дозволених цілей, вони повинні випускатися з інструкціями по вимогам безпеки зони і з надзвичайних процедурам.

Доступ до зон, де обробляється або зберігається важлива інформація, повинен управлятися і бути обмежений тільки повноважними особами. Для більш надійного захисту важливої інформації за можливості необхідно застосовувати засоби управління аутентифікацією, щоб дозволяти і підтверджувати будь-який доступ. Також з цією метою необхідно вести контрольний журнал всього доступу, який повинен міститися в надійному місці.

В зонах особливо жорсткого режиму доступу (секретності) від усіх службовців, підрядників та користувачів третьої сторони і від всіх відвідувачів треба вимагати носити деяку форму видимого ідентифікаційного документа, і вони повинні негайно повідомляти керівника відповідного структурного підрозділу або відповідальну особу, якщо вони стикаються з відвідувачами без супроводжуючого і з будь-ким, хто не носить видимого ідентифікаційного доку-мента.

Персоналу допоміжних служб третьої сторони повинен бути наданий обмежений доступ в зони безпеки або до засобів обробки важливої інформації тільки тоді, коли потрібно; цей доступ повинен бути дозволений і повинен постійно контролюватися.

Права доступу в зони безпеки повинні регулярно аналізуватися і оновлюватися, і скасовуватися, якщо необхідно.

4.3. Захист офісів, кімнат і засобів

Необхідно застосовувати фізичний захист офісів, кімнат і засобів. Для того, щоб захистити офіси, кімнати та засоби, потрібно розглянути наступні керів-

ні вказівки:

- мають бути враховані відповідні норми і стандарти з техніки безпеки і охорони праці;

- ключові засоби мають бути розташовані так, щоб уникнути доступу до них широкому загалу;

- там, де це може бути застосовано, будівлі мають бути скромними і повинні давати мінімальну вказівку на їх мету, без яскравих написів, зовні будівлі або всередині неї, що вказують на наявність видів діяльності з обробки інформації;

- покажчики і внутрішні телефонні книги, що вказують на місця розташування засобів обробки важливої інформації, не повинні бути легко доступні широкому загалу.

4.4. Захист від зовнішніх і екологічних загроз

Повинен застосовуватися фізичний захист проти збитку від вогню, повені, землетрусу, вибуху, громадських заворушень та інших форм природ-ного або штучного лиха.

Увага повинна бути приділена будь-яким загрозам порушення безпеки, які представляють сусідні приміщення, наприклад, вогонь в сусідньому приміщенні, витік води з даху або в перекриттях нижче рівня землі, або вибух на вулиці.

Наступні керівні вказівки мають бути розглянуті для того, щоб уникнути шкоди від вогню, повені, землетрусу, вибуху, громадських заворушень та ін-ших форм природного або штучного лиха.

Небезпечні або горючі матеріали повинні зберігатися на безпечній відстані від безпечної зони. Несортована продукція, така як канцтовари, не повинна зберігатися в безпечній зоні.

Резервне обладнання та резервні копії повинні бути розташовані на безпечній відстані для того, щоб уникнути шкоди від лиха, що впливає на основне місце розташування.

Має бути передбачено і відповідним чином розміщене протипожежне обладнання.

4.5. Робота в безпечних зонах

Повинні бути розроблені і застосовуватися фізичний захист і керівні вказівки для роботи в безпечних зонах.

Персонал повинен бути обізнаний про існування безпечної зони або про діяльність в безпечній зоні тільки на основі принципу службової необхідності.

Треба уникати бездоглядності роботи в безпечних зонах, як з причин безпеки, так і для того, щоб запобігти можливості для зловмисної діяльності.

Порожні безпечні зони повинні фізично замикатися і періодично перевірятися.

Фотографічне, відео, аудіо або інше записуюче обладнання, таке як камери на мобільних пристроях, не повинні допускатися, якщо тільки не дозволено.

Організація роботи в безпечних зонах включає засоби управління для

службовців, підрядників та користувачів третьої сторони, що працюють в безпечній зоні, а також іншу діяльність третьої сторони, яка відбувається там.

4.6. Зони відкритого доступу, поставки й відвантаження

Місця доступу, такі як зони поставки і відвантаження, а також інші місця, де сторонні особи можуть проникнути в приміщення, повинні керуватись і, якщо можливо, повинні бути ізольовані від засобів обробки інформації, щоб уникнути недозволеного доступу.

Доступ до зон поставки і вантаження зовні будівлі повинні обмежуватися певним і повноважним персоналом.

Зони поставки і вантаження повинні бути спроектовані так, щоб поставки могли бути розвантажені без надання персоналу, який здійснює поставку, доступу до інших частин будівлі.

Зовнішні двері зони поставки і відвантаження повинні охоронятися, коли відкриті внутрішні двері.

Вхідні матеріали повинен бути перевірений на можливі загрози перш, ніж цей матеріал буде переміщений із зони поставки і відвантаження в місце використання;

Вхідний матеріал повинен бути зареєстрований згідно з процедурами управління активами на вході на місце розташування.

Вхідні та вихідні вантажі повинні бути фізично відділені, якщо це можливо.

5. Захист устаткування

5.1. Розташування та захист устаткування

Обладнання повинно бути розташоване або захищене так, щоб знизити ризики виникнення екологічних загроз і небезпек, а також кількість можливостей для недозволеного доступу.

Обладнання повинно бути розташоване так, щоб мінімізувати необов’язковий доступ в робочі зони.

Засоби обробки інформації, які звертаються з важливими даними, повинні розташовуватися так і мати такий кут видимості, щоб знизити ризик того, що інформацію побачать сторонні особи в ході їх використання, а засоби збері-гання повинні охоронятися для того, щоб уникнути недозволеного доступу.

Елементи, що вимагають особливого захисту, повинні бути ізольовані для того, щоб знизити загальний рівень необхідного захисту.

Повинні бути створені засоби управління для того, щоб мінімізувати ризик можливих фізичних загроз, наприклад, крадіжка, пожежа, вибухонебезпечні речовини, дим, вода (або збій в подачі води), пил, вібрації, хімічні впливи, перешкоди електропостачанню, перешкоди зв’язку, електромагнітне випромінювання і вандалізм.

Повинні бути визначені керівні вказівки щодо вживання їжі, напоїв і паління поблизу засобів обробки інформації.

Зовнішні умови, такі як температура і вологість, повинні постійно контро-

люватися на наявність умов, які могли б негативно вплинути на роботу засобів обробки інформації.

Захист від блискавки повинен бути застосований до всіх будівель, і блискавкозахисні фільтри повинні бути встановлені на всі вхідні лінії електропередач і лінії зв'язку.

Обладнання, яке оброблює важливу інформацію, має бути захищене для того, щоб мінімізувати ризики витоку інформації каналами по-бічних випромінювань.

5.2. Допоміжні комунальні служби

Обладнання повинно бути захищене від відмов в системі електропостачання та інших порушень, які викликаються збоями в роботі комунальних служб.

Всі допоміжні комунальні служби, такі як електропостачання, водопостачання, каналізація, опалення, вентиляція і кондиціювання повітря повинні регулярно контролюватися і випробовуватися, з метою забезпечення їх правильної роботи і зниження будь-яких ризиків від їх неправильного функціонування або збою в їх роботі. Повинно бути забезпечено підходяще електропостачання, яке відповідає специфікації обладнання, наданій виробником.

Для устаткування, що підтримує критичні ділові операції, рекомендується використовувати джерела безперебійного живлення (ДБЖ) для того, щоб підтримувати нормальне завершення роботи або безперервну роботу.

Плани дій на випадок аварій в системі електропостачання повинні враховувати дію, яку потрібно зробити у разі збою в роботі ДБЖ. Повинна бути розглянута можливість використання резервного генератора, якщо потрібно продовжувати обробку в разі тривалої перерви в подачі електроенергії.

Повинна бути доступна належна поставка електроенергії (палива) для того, щоб генератор міг працювати тривалий період. Устаткування ДБЖ і генератори повинні регулярно перевірятися для того, щоб гарантувати, що вони володіють необхідною потужністю, і випробовуватися відповідно до рекомендацій виробника. Крім того, треба розглянути можливість використання декількох джерел живлення або, якщо приміщення велике, то окремої електропідстанції. Перемикачі аварійного відключення живлення повинні бути розташовані близько запасних виходів в кімнатах з обладнанням для того, щоб полегшити швидке відключення електроживлення в разі аварійної ситуації. На випадок збою в роботі основної мережі електроживлення повинно бути передбачено аварійне освітлення. Водопостачання повинно бути стабільним, щоб постачати системи кондиціонування повітря, зволожуючого обладнання та системи пожежогасіння (там, де використовуються). Неправильна робота системи водопостачання може пошкодити обладнання або перешкодити результативній роботі системи пожежогасіння. Якщо потрібно, то повинна бути оцінена і встановлена система сповіщення для того, щоб виявляти збої в допоміжних комунальних службах. Телекомунікаційне обладнання має бути підключене до постачальника комунальних послуг, принаймні, двома різними маршрутами, щоб зменшити збої в роботі одного шляху сполучення.

Можливості досягнення безперервності електропостачання включають розподілене живлення для того, щоб уникнути однієї критичної точки в електропостачанні.

5.3. Захист кабельних з'єднань

Силові кабелі і кабелі віддаленого зв'язку, по яких передаються дані або допоміжні інформаційні послуги, повинні бути захищені від перехоплення або ушкодження.

Для забезпечення безпеки кабельних з'єднань повинні бути розглянуті наступні керівні вказівки.

Силові лінії та лінії далекого зв'язку, що входять в засоби обробки інформації, повинні бути підземними там, де це можливо, або повинні підля-гати альтернативному захисту.

Мережеві кабелі повинні бути захищені від недозволеного перехоплення або пошкодження, наприклад, шляхом використання кабельного каналу або уникнення маршрутів, що пролягають через загально-доступні зони.

Силові кабелі мають бути відокремлені від кабелів далекого зв'язку для того, щоб запобігти перешкодам.

Легкопомітне маркування кабелів і устаткування повинні використовуватися для того, щоб мінімізувати помилки через неправильне поводження, такі як випадкова комутація неправильних мережевих кабелів.

Для того, щоб знизити можливість помилок, повинен використовуватися документований список комутацій.

Для важливих або критичних систем, додаткові засоби управління, які треба розглянути, включають в себе наступне:

- установка броньованого кабельного каналу і замкнених кімнат або блоків в контрольних точках і точках переривання;
- використання альтернативної маршрутизації та / або засобів передачі даних, що забезпечують відповідний захист;
- використання оптоволоконного кабелю;
- використання електромагнітного екранізування для захисту кабелю;
- ініціація технічних зачисток («зачистка» [sweep] - обстеження приміщень та об'єктів з метою виявлення приховано встановлених пристроїв негласного знімання інформації) і фізичного контролю на предмет наявності недозволених приладів, підключених до кабелю;
- контрольований доступ до комутаційних панелей і кабельних кімнат.

5.4. Обслуговування обладнання

Обладнання повинно правильно обслуговуватися для забезпечення безперервної доступності та цілісності.

Для обслуговування обладнання повинні бути розглянуті наступні керівні вказівки:

- обладнання повинно обслуговуватися відповідно до рекомендованої постачальником періодичністю і специфікаціями технічного обслуговування;
- тільки повноважний обслуговуючий персонал повинен виконувати

ремонт і обслуговувати обладнання;

- повинні зберігатися записи про всі передбачувані або фактичні дефекти, а також про всі запобіжні та коригувальні обслуговування;

- якщо обладнання включено в графік обслуговування, то повинні бути реалізовані відповідні засоби управління, що враховують, чи виконується це обслуговування місцевим персоналом або персоналом, зовнішнім по відношенню до організації; якщо це необхідно, то обладнання має бути очищено від важливої інформації;

- всі вимоги, накладені страховими полісами, повинні бути виконані.

5.5. Захист обладнання, що знаходиться за межами робочого місця

Захист повинен застосовуватися для обладнання, що знаходиться за межами робочого місця, з урахуванням різних ризиків роботи за межами організаційних приміщень.

Незалежно від власності, використання будь-яких засобів обробки інформації за межами організаційних приміщень повинно бути дозволено керівництвом.

Для захисту обладнання, що знаходиться за межами робочого місця, повинні бути розглянуті наступні керівні вказівки.

Обладнання і носії інформації, що виносяться з приміщень, не повинні залишати без нагляду в загальнодоступних місцях. Портативні комп’ютери при подорожі повинні перевозитися в якості ручної поклажі і повинні бути замасковані, якщо можливо;

Весь час повинні дотримуватися інструкції виробника для захисту обладнання, наприклад, захист від сильних електромагнітних полів.

Засоби управління домашньою роботою повинні бути визначені оцінкою ризику, і відповідні засоби управління повинні бути застосовані, наприклад, політика чистого столу, засоби управління доступом для комп’ютерів і безпечний зв’язок з офісом.

Ризики порушення системи безпеки, наприклад, ризик збитку, крадіжки або підслуховування, можуть значно відрізнятися в залежності від місця розташування і повинні бути враховані при визначенні найбільш придатних засобів управління.

Обладнання, що використовується для зберігання і обробки інформації, включає всі форми персональних комп’ютерів, органайзерів, мобільних телефонів, смарт-карт, паперів або іншу форму, яка тримається для домашньої роботи або несеться з місця роботи.

5.6. Безпечна ліквідація або повторне використання обладнання

Всі елементи обладнання, що містять носії інформації, повинні бути перевірені для забезпечення того, що будь-які важливі дані і ліцензійне програмне забезпечення було видалено або надійно затерті перед ліквідацією.

Пристрої, що містять конфіденційну інформацію, повинні бути фізично знищені, або інформація повинна бути знищена, видалена або затерта, використовуючи відповідні методи з метою зробити оригінальну інформацію не-

відновною, замість того, щоб використовувати стандартну функцію видалення або форматування.

Пошкоджені пристрої, що містять важливі дані, можуть потребувати оцінку ризиків для того, щоб визначити, чи повинні елементи бути знищені фізично, відправлені для ремонту або забраковані.

Інформація може бути розголошена за допомогою недбалої ліквідації або повторного використання устаткування.

5.7. Винос майна

Обладнання, інформація чи програмне забезпечення не повинні виноситися за межі робочого місця без попереднього дозволу.

Службовці, підрядники та користувачі третьої сторони, які мають повноваження вирішувати винос активів за межі робочого місця, повинні бути чітко визначені.

Мають бути встановлені обмеження на час виносу обладнання, і після повернення обладнання має бути перевірено на відповідність.

Якщо це необхідно і доречно, то обладнання повинно бути записане, як винесене з робочого місця і записане після повернення.

Раптові перевірки, що вживаються з метою виявити недозволений винос майна, також можуть проводитися для того, щоб виявити недозволені записуючі пристрої, зброю та інше, і запобігти їх внесенню на робоче місце. Такі раптові перевірки повинні виконуватися згідно з відповідними законами і нормами. Люди повинні бути проінформовані про те, чи проводяться раптові перевірки, та перевірки повинні виконуватися тільки з дозволом, відповідно до вимог закону та юридичних вимог.

Керуючий справами виконкому ***Олександр Гижко***