Додаток
до розпорядження голови
районної в місті ради
від 09.11.2017 № 239-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 9001:2009.

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 9001:2009 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 перетворення, 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 ***О.Гижко***