Додаток
до розпорядження голови
районної в місті ради
від 09.11.2017 № 243-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 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.

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 замкнені, коли знаходяться без нагляду, і повинен бути врахований зовнішній захист 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 знадобитися 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 документа.

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 то-

го, щоб захистити офіси, кімнати та засоби, потрібно розглянути наступні керівні 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 природного 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 інших 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 зберігання 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 контролюватися 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 підлягати 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, вико-

ристовуючи відповідні методи з метою зробити оригінальну інформацію невідновною, 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 ***О.Гижко***