Додаток 1
до розпорядження голови
районної в місті ради
від 09.11.2017 № 241-р

Політика
у сфері інформаційної безпеки
виконкому Довгинцівської районної в місті ради

І. 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.

ІІ. 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.

ІІІ. 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 ***О.Гижко***

Додаток 2
до розпорядження голови
районної в місті ради
від 09.11.2017 № 241-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 маркування 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 ідентифікація процесів виконується представниками робочої змішаної групи (управлінці, фахівці з інформаційних систем і користувачі).

Зазвичай первинні активи - це основні процеси та інформаційна діяльність 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 зґбезпечення);
- 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. Наприклад, можна визначити коефіцієнт цінності різних категорій інформації, відображених у таблиці 2.

Таблиця 2
Коефіцієнт цінності інформації

Категорія інформації	***Відкрита інформація***	***Конфіденційна інформація***			
		Управлінська	***Технологічна***	***Фінансова, бухгалтер.***	***Персональні 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 використовуються 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 ***О.Гижко***

Додаток 1

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 обладнанням (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'язковим 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 інформаційної 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).