распределения ВИ по группам применения с помощью предложенной методики и данные распределения ВИ по группам применения с помощью традиционной методики полностью совпадают. Предложенная методика контроля работоспособности ВИ (с учётом относительной простоты и дешевизны её реализации) может быть использована для отбора ВИ по группам применения как в условиях производства (например, при выходном контроле), так и у потребителя (при входном контроле).

IV Выводы

1. Сравнительная оценка относительных октавных уровней виброускорения при проверке ВИ с помощью ВШВ и с помощью компьютерной программы Spectra Plus анализатора спектра звукового диапазона показала, что вид корреляционных областей и полученные значения коэффициентов корреляции двух групп показаний дают основания считать правомерным использование указанной программы для сравнительной оценки относительных октавных уровней виброускорения.

2. Применение программы Spectra Plus для сравнительной проверки чувствительности ВД, подключаемых непосредственно к звуковой карте, показало, что ВД, представляющий собой ВИ типа ОЦЗІ-ВА/В в режиме прямого пьезоэффекта, обладает (по сравнению со стандартными ВД типа ВПИ-100, ДН-3, ДН-4) чувствительностью, которая позволяет подключать его ко входу звуковой карты без дополнительного усилителя.

3. Сравнительное исследование относительных уровней виброускорения при наличии между ВД и проверяемым ВИ промежуточной стандартной массы, а также при прямом контакте рабочих поверхностей ВД и проверяемого ВИ, показало, что вид корреляционных областей и полученные значения коэффициента корреляции двух групп показаний подтверждают правомерность использования прямого контакта рабочих поверхностей ВД и проверяемого ВИ при сравнительной оценке работоспособности ВИ.

4. Контроль работоспособности ВИ может быть осуществлён с помощью методики, согласно которой рабочая поверхность проверяемого ВИ, подключённого к выходу виброакустического генератора, имеет непосредственный контакт с рабочей поверхностью ВД, представляющего собой ВИ, подключённый непосредственно ко входу звуковой карты ПК. Критерием работоспособности проверяемого ВИ является его принадлежность к одной из групп применения, чему соответствует расположение огибающей спектра регистрируемого сигнала в границах поля допуска для конкретной группы применения.

Литература: ***1.*** *НДТЗИ Р-001-2000. Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації.* ***2.*** *Порошин И., Сигаев А., Непочатых Ю. Обеспечение комфортности выделенных помещений при использовании систем активной виброакустической защиты. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К., вип.(1)12, 2006, с. 100-106.* ***3.*** *Гмурман В. Е. Теория вероятностей и математическая статистика – М.:Высшая школа, 2004. – 479 с.*

УДК: 004.052.2+004.056

ОРГАНІЗАЦІЙНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСУ ВІДНОВЛЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ПІСЛЯ АВАРІЇ

Любомир Пархуць, Тетяна Хома, Олена Хмиз
Національний університет «Львівська політехніка»

Анотація: **Багато організацій не зможуть успішно функціонувати, якщо стають недоступними послуги їх інформаційно-комунікаційних систем. У роботі проведено аналіз підходів у забезпеченні відмовостійкості інформаційних систем, подано порівняльну характеристику існуючих організаційних заходів а також відомих засобів технічної підтримки процесу відновлення інформаційних систем після аварії. Описано завдання плану відновлювальних робіт після аварії та розкрито зміст резервування систем і даних. Проаналізовано доступність в Україні таких послуг як IT-аутсорсинг та IT-консалтинг. Відзначено потребу у створенні системи підтримки прийняття рішень для проведення відновлювальних робіт.**

Summary: **Many businesses could not continue to operate successfully if their IT services were unavailable for a period of time. In this article approach to IT systems fault tolerance is analyzed, existing organizational activities as well as means of technical support for IT system backup are compared. Disaster recovery plan, system and data reservations are described. Availability of IT-outsourcing and IT-consulting services in Ukraine are analyzed. Need in decision-making system for recovery activities are mentioned.**

Ключові слова: **Інформаційно-комунікаційна система, інцидент інформаційної безпеки, план відновлення після аварії, резервування систем і даних, реплікація даних, IT-аутсортсинг, система підтримки прийняття рішень.**

I Вступ

Початок третього тисячоліття ознаменувався проникненням комп'ютерних інформаційних технологій (ІТ) не лише у такі сфери як освіта, управління, мас-медіа, але також у різні «матеріальні» галузі економіки, банківської діяльності, торгівлі, транспорту тощо. Наразі будь-яка професійна діяльність вимагає інформаційної підтримки, тому організації створюють інформаційну інфраструктуру у вигляді інформаційно-комунікаційних систем (ІКС). Використання ІКС забезпечує організації оперативність і ефективність управлінських рішень, конкурентність на ринку та низку інших переваг. Разом з тим комп'ютеризація має також і великий негативний наслідок – узалежнення діяльності організацій від інформаційної інфраструктури. Склалася ситуація, коли збої у роботі ІКС створюють перешкоди у інформаційному забезпеченні робочого процесу, а відтак безпосередньо негативно позначаються на функціонуванні організації, співпраці із діловими партнерами та клієнтами.

У цьому сенсі особливо катастрофічними за своїми наслідками є аварії інформаційних систем, які можуть призвести не лише до тривалих простоїв, але і до втрати критичних даних. На жаль, створення абсолютно безпечної ІКС є неможливим через повну втрату її функціональності, тому навіть у захищених системах завжди існує залишковий ризик [1 – 3]. Це означає, що попри створення системи захисту інформації можуть виникати інциденти інформаційної безпеки і навіть аварії інформаційної системи. Тому заздалегідь створений та відповідно організаційно і технічно забезпечений план аварійного відновлення ІКС здатний пом'якшити наслідки аварії і в підсумку зменшити фінансові та інші ризики організації.

Як у світовій практиці, так і в Україні завдання підтримки прийняття рішень й автоматизації керування аваріями інформаційних систем потребує подальшого дослідження. В жодному з міжнародних чи вітчизняних нормативно-технічних документах, які частково або повністю присвячені керуванню інцидентами інформаційної безпеки і аварій ІКС, не визначено, що саме можна/треба розуміти під автоматизацією процесу, з яких функцій і елементів ця автоматизація повинна складатися та як її проводити.

Метою роботи є характеристика аварії в контексті функціонування інформаційної системи, формулювання завдань плану відновлення після аварії, опис існуючих рішень із ефективного обслуговування аварійних ситуацій, а також обґрунтування доцільності розроблення та використання при управлінні аваріями в ІКС системи підтримки прийняття рішень.

II Аварія як можливий стан інформаційно-комунікаційних систем

Інформаційно-комунікаційна система – це організаційно-технічна система, яка реалізує певну технологію оброблення та передавання інформації для задоволення інформаційних потреб користувачів [1].

Можна виділити три життєві цикли ІКС: створення, функціонування і утилізація (регламентована ліквідація ІКС). Державний стандарт [4] розрізняє вісім стадій створення ІКС: формування вимог до інформаційної системи; розробка концепції; технічне завдання; ескізний проект; технічний проект; робоча документація; введення в експлуатацію; супроводження.

Навіть за правильного конфігурування і коректного адміністративного супроводження в тракті експлуатації інформаційно-комунікаційної системи через невиявлені вразливості та реалізацію загроз може порушитися її нормальний стан, внаслідок чого ІКС перейде до нештатного режиму (рис. 1). Нештатний режим можна описати як стан інциденту інформаційної безпеки або як аварійний стан. Згідно з означенням, прийнятим в ITIL (Information Technology Infrastructure Library), під інцидентом розуміють будь-яку подію, що не є елементом нормального функціонування служби і при цьому надає або здатна зробити вплив на роботу служби шляхом її переривання або зниження якості [3, 5].

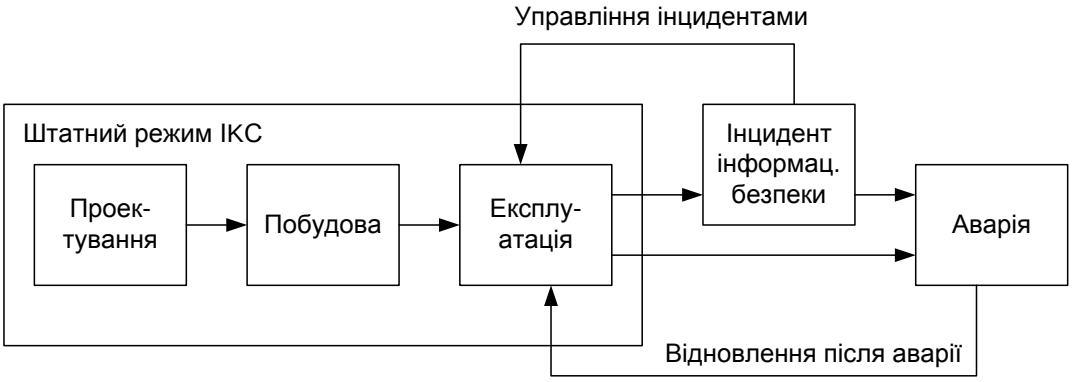

Рисунок 1 – Місце аварії в контексті функціонування ІКС

У ІКС, як і в будь-якій іншій системі, є можливим виникнення аварії. Аварія – це неочікуване пошкодження чи вихід з ладу, що стався з техногенних (конструктивних, технологічних, експлуатаційних) або природних причин [6]. В інформаційно-комунікаційній системі під терміном «аварія» розуміють значне пошкодження, тобто вихід з ладу обладнання, що призводить до відмови цілої ІКС, а відтак блокування роботи користувачів, порушення робочого процесу організації і значних матеріальних і фінансових збитків**.**

Проте слід зазначити, що не завжди інциденти є причиною аварій у інформаційній системі. Інколи інциденти можуть стати джерелом вразливостей, які зловмисник зможе використати, щоб завдати шкоди системі, знизити ефективність її функціонування, завдати матеріальних та фінансових втрат. Наприклад, використовуючи залишений без нагляду незаблокований комп'ютер зловмисник може викрасти інформацію, що є порушенням конфіденційності, але це не створить аварійну ситуацію у ІКС, оскільки вона не вийде з ладу.

Таким чином, у процесі експлуатації інформаційна система може перебувати у нормальному (штатному) режимі, а також у стані інциденту інформаційної безпеки та аварійному стані. Якщо проаналізувати статистику загроз інформаційної безпеки, які найчастіше реалізуються, приводячи ІКС до нештатного режиму, то це насамперед є інциденти з причин помилок персоналу і тільки за ними йдуть атаки зловмисників. При цьому, якщо інцидент лише знижує якість функціонування інформаційної системи і може призвести до передаварійного стану, то аварія означає відмову функціонування ІКС через руйнування апаратних засобів чи пошкодження програмного забезпечення.

Щодо надзвичайних подій техногенного, природного або іншого характеру, які здатні частково або повністю знищити ІКС організації, то вони, на щастя, трапляються нечасто. Але в сучасних умовах вся діяльність організації може виявитися під загрозою, якщо дії персоналу в критичній ситуації не було продумано заздалегідь. Для мінімізації ризиків необхідні катастрофостійка інформаційна інфраструктура, технології захисту даних, навчений персонал і план аварійного відновлення інформаційної системи [7].

Відмова інформаційної системи зумовлює прямі та опосередковані збитки для організації, а її відновлення вимагає часових та фінансових затрат. У деяких випадках кошти на відновлення ІКС є сумірними із затратами на її створення. Тому важливо розглянути можливі шляхи підвищення ефективності робіт із відновлення ІКС.

Аналіз літературних джерел показав, що на цей час для забезпечення безперервності ІТ-послуг застосовуються як організаційні заходи, так і технічні засоби забезпечення аварійностійкості інформаційно-комунікаційних систем.

ІІІ Завдання аварійного планування та стадії відновлювальних робіт після аварії ІКС

План відновлення після аварії (*disaster recovery plan, DRP*) - це опис дій працівників у аварійній ситуації, коли програмне забезпечення або обладнання повністю несправне упродовж тривалого часу. Він дає змогу звести до мінімуму наслідки аварії і забезпечує можливість максимально швидко взяти під контроль та відновити виконання критично важливих завдань.

Головне завдання аварійного планування – реалізація заходів, націлених на локалізацію аварії, пом'якшення її наслідків і якнайшвидше повернення ІКС до нормального функціонування. План аварійного відновлення містить докладний перелік заходів і дій, які необхідно виконати «до», «під час» і «після» виникнення надзвичайної ситуації. Тут визначається порядок повідомлення відповідальних співробітників та викладаються детальні інструкції для виконавців. Все це дозволяє максимально швидко відновити

працездатність ІКС. Прийнятний для роботи час відновлення є одним із ключових факторів, від якого залежить вибір стратегії резервування обладнання й способу реплікації даних. Понад третини західних компаній фінансового сектора мають аварійні плани з регламентним часом відновлення менше 4 годин [8].

У процесі реалізації програм забезпечення безперервності функціонування ІКС приділяють особливу увагу процедурам тестування розроблених регламентів з метою перевірки їхньої ефективності. Запровадження плану відновлення після аварії має супроводжуватися заходами щодо навчання персоналу й перевіркою готовності всіх служб організації до надзвичайної ситуації. Регулярні перевірки й навчання дають можливість переконатися в адекватності й ефективності розробленого плану і гарантують, що у випадку аварії персонал виконає всі необхідні дії [8].

Розглядаючи відновлювальні роботи як процес, можна виділити такі стадії (див. рис. 2).

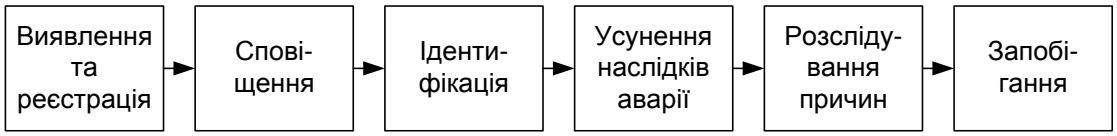

Рисунок 2 – Стадії процесу відновлення ІС після аварії

Виявлення та реєстрація аварії повинна здійснюватись відповідальною особою, адміністратором, користувачем чи співробітником за інструкцією, що чітко окреслює його дії. Звіт про виявлення та реєстрацію аварії має містити докладний опис аварії, перелік залучених співробітників, прізвище співробітника, що зафіксував аварію, дату виникнення та реєстрації.

Сповіщення відповідальних осіб, насамперед фахівців з безпеки і адміністраторів ІТ-сервісів про аварію, що сталася в інформаційній системі. Список осіб в організації, яких потрібно повідомити у випадку аварії, доцільно оформити на стенді. Це пришвидшує роботу персоналу під час аварії. Також необхідно сповістити користувачів ІКС про стан інформаційної системи і очікуваний час її відновлення.

Ідентифікація є основою будь-яких систем захисту, в тому числі і ІКС. Завданням ідентифікації є структурно-просторова локалізація джерела небезпеки, рівень критичності аварії, можливий збиток та ін. параметри, необхідні для вирішення конкретного завдання. Лише ідентифікувавши аварію можна застосувати адекватні засоби і заходи її подолання.

Усунення наслідків аварії включає опис дій, які необхідно виконати для локалізації деструктивних впливів аварії та її подолання (конкретні дії для кожного виду аварії), а також терміни, упродовж яких слід усунути наслідки і причини аварії. Терміни їх усунення залежать від рівня аварії. Слід заздалегідь розробити інструкцію щодо блокування тієї чи іншої аварії та паспорт ліквідації наслідків аварії, який містить конкретні кроки відновлювальних робіт.

Таким чином, інструкція щодо усунення наслідків і причин аварії може включати: процедуру визначення рівня критичності аварії, опис дій, які виконуються для усунення наслідків і причин аварії, терміни усунення і примітки, що окреслюють міру відповідальності за недотримання інструкції.

Розслідування причин аварії включає в себе визначення порушень правил користування ІКС, здійснення аналізу причин, що призвели до нештатної ситуації, збір доказів, визначення відповідних дисциплінарних стягнень, покарання винних у їх виникненні. У великих організаціях, як правило, призначають комісію для розслідування аварій інформаційної системи (до складу якої може входити співробітник, який реєструє аварії). Інструкція щодо розслідування причин аварії повинна описувати: дії щодо розслідування аварії (у тому числі визначення винних в його виникненні), причини виникнення, правила збору, зберігання доказів і правила винесення дисциплінарних стягнень.

Запобігання аварії у майбутньому передбачає реалізацію низки заходів щодо ліквідації причин аварії, зменшення виявлених вразливостей компонент ІКС. За рахунок аналізу аварій в ІТ-системі підвищується ймовірність запобігання майбутнім аваріям, поліпшуються механізми і процеси забезпечення інформаційної безпеки.

IV Резервування ресурсів ІКС та резервне зберігання даних

На цей час окрім розглянутих вище організаційних заходів із планування відновлювальних робіт задля забезпечення неперервності функціонування своїх ІКС організації можуть застосовувати низку рішень із арсеналу аварійностійких (катастрофостійких) технологій. За своєю суттю ці технології передбачають *резервування ресурсів інформаційної системи* та *резервне зберігання даних*.

Можна виділити кілька рівнів резервування ресурсів інформаційної системи залежно від її значимості для діяльності організації, а також від чутливості діяльності до часу простою ІКС. Прикладом найнижчого рівня

резервування для ІКС другорядного значення може бути просто серверна площадка, обладнана необхідними інженерними системами й підготовлена для установки серверного устаткування. Такий підхід дозволяє відновити роботу системи протягом декількох днів. Для більш важливих інформаційних систем відокремлений обчислювальний центр повинен містити все необхідне устаткування, щоб у випадку катастрофи можна було швидко запустити резервну систему (холодне резервування). А для найбільш критичних систем додатково необхідні системи реплікації даних і плани аварійного відновлення, що забезпечують збереження даних і безперервність функціонування ІКС (гаряче резервування) [7].

Іншою складовою аварійностійких технологій, що стосується інформаційних ресурсів є резервування даних. У надзвичайних ситуаціях найбільший збиток організації наносять не тимчасова неможливість доступу до критичних даних, а цілковита їх втрата. Мінімізація цього ризику досягається за рахунок резервного копіювання й реплікації даних. На рис. 3 наведено класифікацію методів резервування даних.

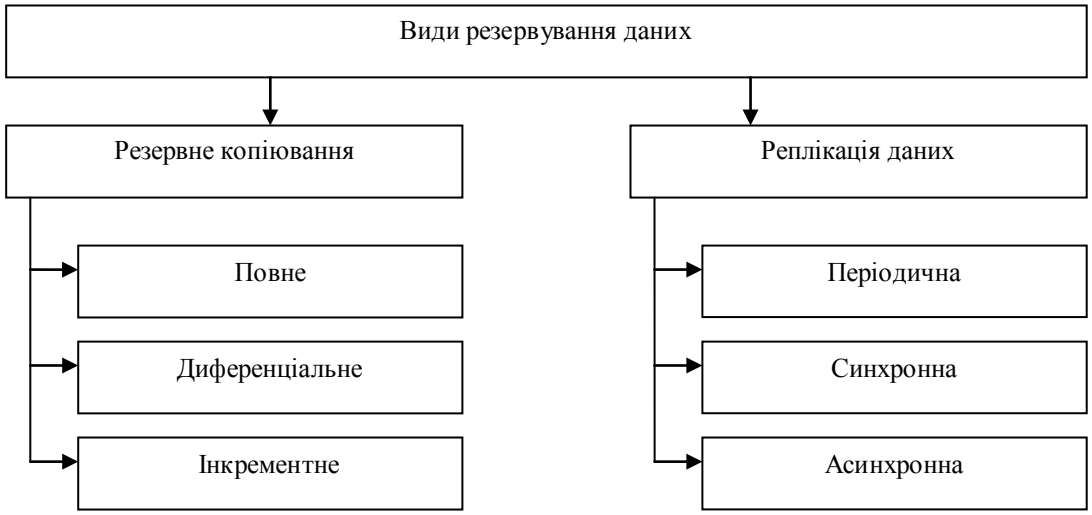

Рисунок 3 – Рівні резервування інформаційних систем

Резервне копіювання (*англ. backup*) - процес створення копії даних на спеціальних носіях (стримерах, матрицях дисків і т. д.), призначений для відновлення даних в основному місці їх розташування в разі їх пошкодження або руйнування [8]. Резервне копіювання необхідне для швидкого і недорогого відновлення інформації (документів, програм) у випадку втрати робочої копії інформації з будь-якої причини. Важливо зберігати носії з резервними копіями окремо від оригінальних даних.

Повне резервування (*full backup*) зазвичай зачіпає всю операційну систему і всі дані. Створення щотижневих, щомісячних і щоквартальних архівів передбачає повне резервування. Перше щотижневе архівування повинно бути повним резервуванням, що зазвичай виконується по п'ятницях або упродовж вихідних, і передбачає копіювання всіх бажаних файлів. Подальші резервування, які проводять з понеділка по четвер аж до наступного повного резервування, можуть бути інкрементними або диференціальними, щоб заощадити час і місце на носії. Повне резервування слід проводити, принаймні, щотижня.

Диференціальне або *різницеве резервування* (*differential backup*) передбачає копіювання кожного файлу, зміненого з моменту останнього повного резервування. Диференціальне резервування прискорює процес відновлення і для відновлення вимагає лише останню повну і останню диференціальну резервні копії. Популярність диференціального резервування зростає, оскільки всі копії файлів виконуються в певні моменти часу, що, наприклад, дуже важливо при зараженні ІКС вірусами.

Інкрементне або *додаткове резервування* (*incremental backup*) передбачає копіювання тільки тих файлів, які були змінені з часу останнього повного або додаткового резервного копіювання. Подальше додаткове резервування додає тільки файли, які були змінені з моменту попереднього додаткового резервування. Таке резервування займає менше часу, оскільки копіюється менша кількість файлів. Однак, процес відновлення даних займає більше часу, тому що повинні бути відновлені дані останнього повного резервування, плюс дані всіх наступних додаткових резервувань. При цьому, на відміну від диференціального резервування нові або змінені файли не заміщають старі, а додаються на носій незалежно.

Реплікація даних – це віддалене резервне копіювання, що на відміну від звичайного резервного копіювання передбачає виділення таких додаткових ресурсів, як віддалені системи архівування, що з'єднані

із ІКС організації каналами зв'язку. Розмаїтість схем і варіантів реплікації даних забезпечує можливість вибору найбільш ефективного й раціонального рішення для кожного конкретного завдання.

Періодична реплікація або *реплікація за розкладом* допомагає зберегти у відокремленому центрі копію даних на фіксований момент часу в минулому. Основний недолік цього методу – втрата актуальності даних за період часу, що дорівнює інтервалу між реплікаціями. Проте, реплікація за розкладом є доволі ощадливим рішенням для організацій, коли час відновлення не є критично важливим, а також допускається незначна втрата даних.

Синхронна реплікація гарантує найвищий рівень надійності, забезпечуючи ідентичність всіх копій даних. Висуваючи високі вимоги до каналів зв'язку, синхронна реплікація найчастіше застосовується для найбільш важливих застосувань, де необхідний максимальний захист даних.

Асинхронна реплікація забезпечує безперервність передачі даних, причому навіть в умовах нестабільності каналів зв'язку. Цей спосіб допомагає зберегти високу продуктивність інформаційних систем і контролювати завантаження каналів передачі даних, але не забезпечує настільки ж високий рівень актуальності даних, як синхронна реплікація.

Останнім часом часто застосовуються схеми множинної реплікації, коли дані передаються з основного обчислювального центра відразу до кількох резервних центрів. Нерідко в цих випадках навіть застосовуються різні способи реплікації для більш надійного й комплексного захисту даних.

Реплікація даних має деякі переваги порівняно з традиційними методами резервного копіювання:

- віддалене копіювання не вимагає участі користувачів та забезпечує необмежене в часі зберігання даних;
- деякі віддалені резервні служби можуть працювати безперервно, копіюючи зміни у файлах.

Проте реплікація має й кілька істотних недоліків:

- відновлення даних може бути повільним, за обмеженої смуги пропускання каналів зв'язку;
- постачальники послуг віддаленого резервного копіювання можуть не надавати гарантій конфіденційності, тому організації-клієнти повинні самостійно шифрувати дані для віддаленого зберігання, при цьому, якщо ключ шифрування буде втрачено, то відновлення даних стане неможливим;
- деякі постачальники послуг реплікації часто мають щомісячні ліміти, які внаслідок чого обсяги резервного копіювання для організацій можуть обмежуватися.

Надійне збереження дуже важливих даних у випадку виникнення надзвичайної ситуації забезпечується за допомогою розподілених мереж зберігання даних (англ. Storage Area Network – SAN), для роботи яких необхідні надійні й високопродуктивні канали передачі даних. Технологія SAN забезпечує відмовостійкий доступ серверів до ресурсів зберігання і дозволяє знизити сукупну вартість утримання IT-інфраструктури за рахунок оптимального онлайнового управління доступу серверів до ресурсів зберігання. Розподілені мережі зберігання даних складаються з серверів резервного копіювання, системи управління та комунікаційної інфраструктури, що забезпечує фізичний зв'язок між елементами мережі зберігання даних. Подібна архітектура дозволяє забезпечити безперебійне і безпечне зберігання даних, а також обмін даними між елементами мережі зберігання даних. В основі концепції SAN лежить можливість з'єднання будь-якого з серверів з будь-яким пристроєм зберігання даних, що працює за протоколом Fibre Channel. Зручні засоби адміністрування SAN дають можливість скоротити чисельність обслуговуючого персоналу, що знижує вартість зберігання даних.

Об'єднання SAN за допомогою IP-мереж має меншу продуктивність, але за рахунок широкої поширеності й низької вартості IP-каналів цей варіант є більш доступним. Мережі зберігання даних із застосуванням технологій DWDM (системи з хвильовим ущільненням каналів) забезпечують передачу даних на великі відстані з високою швидкістю. У рішеннях цього класу використовуються волоконно-оптичні лінії зв'язку, в тому числі існуючі мережі глобальних операторів зв'язку. Висока швидкість передачі даних по SAN (200 Мбайт/с) дозволяє в реальному часі переміщати дані, що змінюються, у віддалене сховище [7].

V Аутсорсинг центрів оброблення даних. IT-консалтинг

У сучасному розумінні *центр обробки даних* (*ЦОД*) або інша назва *дата-центр* (*data center*) – це комплексне організаційно-технічне рішення, що призначене для створення високопродуктивної, відмовостійкої інформаційної інфраструктури і включає обладнання для обробки і зберігання даних, а також забезпечує підключення до швидкісних каналів зв'язку. *Аутсорсинг* (*outside-resource-using*) – це використання зовнішнього ресурсу, тобто передача організацією на основі довгострокових контрактів деяких виробничих функцій на обслуговування іншій компанії, що спеціалізується у відповідній області. Найбільш комплексна послуга IT-аутсорсингу – це аутсорсинг інформаційних систем [9].

Для створення власної IT-інфраструктури з нуля організаціям потрібні великі кошти і високооплачувані IT-фахівці. Оренда інфраструктури дата-центру забезпечує доступ до новітніх технологій, дає можливість

швидкого розгортання офісів з можливостями нарощування ресурсів. Для багатьох компаній надійність безперебійного функціонування обладнання та мережевої інфраструктури стає сьогодні критичним фактором для функціонування бізнесу. Аутсорсинг IT-інфраструктури дозволяє забезпечити високий рівень надійності даних при обмеженій вартості, надаючи клієнтам можливість оренди серверних стійок і місць в стійці для розміщення обладнання замовника (*co-location*), оренди виділеного сервера (*dedicated server*), ліцензійного програмного забезпечення, каналів передачі даних, а також отримання технічної підтримки [9].

Замовник звільняється від багатьох процедур: технічної підтримки та адміністрування обладнання, організації цілодобової охорони приміщень, моніторингу мережевих з'єднань, резервного копіювання даних, антивірусного сканування програмного забезпечення і т. д. Передаючи свої корпоративні системи на аутсорсинг для резервування, замовники знижують ризик втрати критичної інформації за рахунок використання професійних систем відновлення працездатності IT-систем, а у випадку аварії отримують можливість страхування інформаційних ризиків.

Зазвичай клієнтам ЦОД пропонується декілька рівнів забезпечення безперервності бізнесу. У найпростішому випадку це розміщення резервних систем в дата-центрі з забезпеченням належного захисту. Крім того, може бути варіант, при якому клієнту також надається оренда програмно-апаратних комплексів для резервування. Найбільш повний варіант послуги передбачає розробку повномасштабного плану відновлення систем у разі аварії, який має на увазі аудит інформаційних систем замовника, аналіз ризиків, розробку плану відновлення після аварії, створення і обслуговування резервної копії системи, а також надання обладнаного офісного приміщення для продовження роботи у випадку аварії в основному офісі.

Впровадженню ЦОД в Україні сприяє прийняття законів, що вимагають обов'язкового резервування інформаційних систем. Проте на цей час в Україні працює лише кілька десятків комерційних ЦОД, причому переважна більшість з них розташована в Києві. Найбільш великі дата-центри належать компаніям «Адамант», «Воля», «Датагруп», «Дзвін», Wnet, Imena.UA, «Укртелеком», «Білайн», Newtelco Ukraine, LukyNet, «Комстар-Україна» та ін. Більшість цих компаній (крім Newtelco Ukraine) є одночасно провайдерами Інтернету та інших телекомунікаційних послуг. Перший в Україні дата-центр ColoCall запрацював з 1 серпня 2000 року. На цей час найбільшим спеціалізованим дата-центром України є ЦОД De Novo [9].

Поряд із аутсорсингом ІКС, організаціям також можуть надаватися послуги IT-консалтингу, тобто аутсорсингу IT-персоналу для вирішення різних IT-задач. *IT-консалтинг* – це проектно-орієнтована діяльність, пов’язана з підтримкою бізнес-процесів, що дозволяє дати незалежну експертну оцінку ефективності використання інформаційних технологій.

Можуть надаватися такі послуги IT-консалтингу [9]:

- вибір, проектування та впровадження ІКС із урахуванням вимог інформаційної безпеки;
- аудит ефективності корпоративного IT-забезпечення;
- вдосконалення діяльності IT-підрозділу підприємства або компанії.

Вибір, проектування та впровадження інформаційних систем управління можна застосувати як для окремих структур або підрозділів підприємства або окремих процесів, так і відразу для всього підприємства в цілому, повністю охоплюючи всі сфери його діяльності. Впровадження інформаційних систем для окремих структур може здійснюватися поетапно з подальшим інтегруванням в єдину інформаційно-комунікаційну систему на рівні всього підприємства або компанії, що можливо при розробці правильної IT-архітектури.

Аудит ефективності інформаційних технологій - це послуги з незалежної оцінки стану корпоративного IT-забезпечення, насамперед аналіз ефективності роботи існуючої інформаційної системи, оцінка інформаційних ризиків і рівня безпеки. Послуги щодо вдосконалення діяльності IT-підрозділу підприємства - це вироблення відповідних рекомендацій, розробка концепції розвитку і технічного плану модернізації інформаційної системи. Розробка та впровадження заходів з інформаційної безпеки дозволяє закласти основи для забезпечення надійності ключових процесів в системі і збереження важливої інформації.

Правильно спроектована і розроблена архітектура ІКС володіє модульністю, масштабованістю, гнучкістю, відмовостійкістю, захищеністю та іншими корисними характеристиками, які можуть дати очевидні вигоди: зменшити витрати на розробку, впровадження та підтримку програмного забезпечення, полегшити інтеграцію систем, спростити процес оновлення і заміни елементів ІКС.

VI Висновки

В інформаційному середовищі відбувається багато подій, які потенційно несуть загрозу діяльності організації. Складність та різноманітність інформаційних систем зумовлюють наявність залишкових ризиків незалежно від якості підготовки персоналу, а також від впроваджених заходів і засобів захисту інформації. Також завжди існує ймовірність реалізації нових, невідомих досі загроз інформаційної безпеки. Ці фактори свідчать про ймовірність виникнення аварійних ситуацій в ІКС.

Будь-яка, навіть незначна перерва в діяльності компанії часто повертається для неї втратою клієнтів, зниженням доходів, наносить збиток іміджу і репутації. Для багатьох сучасних фірм неперервність діяльності тісно пов'язана з забезпеченням безперебійної роботи інформаційної системи. Практика показує, що інвестиції в організацію безперебійної роботи ІКС обходяться набагато дешевше, ніж можливі збитки від втрати даних в результаті збою, відмови, аварії.

Хоча аутсортсинг центрів обробки даних є привабливим і перспективним напрямком у забезпеченні аварійностійкості інформаційної інфраструктури, на цей час в Україні його поширення наштовхується на певні труднощі, пов'язані насамперед із недостатньою кількістю ЦОД, недоступністю високоякісних і швидкісних каналів передачі даних для багатьох організацій.

Реалії сьогодення роблять актуальним пошук шляхів із підвищення ефективності організаційно-технічного забезпечення безперебійної роботи власних корпоративних систем. Видається доцільним варіант запровадження в організаціях системи підтримки прийняття рішень у аварійних ситуаціях, яка дасть можливість не тільки обробляти значно більший об'єм інформації, а й значно зменшити вплив психологічних факторів на прийняття необхідних рішень на кожному з етапів відновлення ІКС.

Література: ***1.*** *Гайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем.- К.: Видавнича група BHV, 2009.- 608 с.* ***2.*** *Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов.- М.: Горячия линия – Телеком, 2006.- 544 с.: ил.* ***3.*** *ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою.* ***4.*** *ДСТУ 2941-94. Системи обробки інформації. Розроблення систем. Терміни і визначення.* ***5.*** *Програма інформатизації НАН України. Проект «Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ». Система управління інцидентами інформаційної безпеки.2009.* ***6.*** *Бачинський І. В., Дудикевич В. Б., Зачепило В. С., Пархуць Л. Т., Хома В. В., Яструбецький О. В. Термінологічний словник з інформаційної безпеки // Вид-во „ПАПУГА", Львів:2005. 140 с.* ***7.*** *http://www.jet.msk.su/services_and_solutions/computational_systems/solution_catalog/holocaust_stable_solutions /index.php?print=y.* ***8.*** *Сучасні підходи до побудови катастрофостійких систем зберігання даних (www.sta.gov.ua/doccatalog/document?id=152853).* ***9.*** *Д. Харатишвили. Центры обработки данных: вчера, сегодня, завтра.-"КомпьютерПресс", 2007.-№11.*