УДК 355.02: 396

к.військ.н., доц. **Кацалап В.О.** (НУОУ)
Омельянчук А.В. (ГШ ЗСУ)
Сивак О.В. (ГШ ЗСУ)

DOI: https://doi.org/10.17721/2519-481X/2022/77-04

ОБГРУНТУВАННЯ ПОКАЗНИКІВ ВІДМОВОСТІЙКОСТІ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ЦЕНТРУ ОПЕРАТИВНОГО КЕРІВНИЦТВА ЗБРОЙНИХ СИЛ УКРАЇНИ

Сучасні підходи до обґрунтування показників відмовостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України базуються на тому, що будь-який процес накопичення, збирання та зберігання інформації має незмінно циклічний характер. Ця його сутність обумовлює потребу обґрунтування показників, які дозволяють резервувати дані в автоматизованій системі управління. До таких показників відмовостійкості автоматизованої системи управління центру оперативного керівництва відносяться: цільова точка відновлення – RPO; цільовий час відновлення RTO; безперервності IT-сервісів. Наведені показники визначають ефективність інформаційного забезпечення автоматизованої системи управління, що полягає у забезпеченні керівництва своєчасною та достовірною інформацією.

Зазначене є особливо актуальним в умовах повномасштабної збройної агресії РФ проти України та потребує удосконалення підходів щодо забезпечення відмостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України. Розроблена у статті модель загроз безперервності надання IT-сервісів дозволяє порівняти класи загроз із частотою їх появи та типовими засобами захисту. На їх основі можливо порівнювати відповідні показники регламентного відновлення відносяться, зокрема резервне копіювання та архівування даних на віддаленому сервері (Crossite backup). Крім того, в роботі розглянуті підходи, що базуються на застосуванні фінансових показників ефективності процесів автоматизації (Total cost of ownership), які дозволяють оцінити сукупні витрати на інформаційні технології (обладнання, інструментальні засоби, процеси супроводу інформаційних систем.

Ключові слова: центр, оперативне керівництво, спеціальне програмне забезпечення, відмовостійкість, автоматизована система управління, автоматизовані інформаційні системи, Збройні Сили України.

Вступ. У звіті Департаменту внутрішнього аудиту Міністерства оборони України [1] визначено, що автоматизована системи управління центру оперативного керівництва Збройних Сил України є елементом системи інформатизації Збройних Сил України та складовою частиною Єдиної автоматизованої системи управління військами (силами) і включає процеси створення, впровадження і застосування у різних сферах їх діяльності у мирний та воєнний час сучасних методів, систем і засобів одержання, оброблення, зберігання, передавання та використання інформації.

Процес побудови центру оперативного керівництва є основним елементом сучасної Єдиної автоматизованої системи управління Збройних Сил України та вимагає залучення значних відомчих, людських і матеріальних ресурсів, а досягнення очікуваного ефекту певною, мірою залежить від однакового трактування визначених завдань і розуміння їх складових.

Широкомасштабна агресія РФ проти України показала, що рівень відмовостійкості автоматизованої системи управління центру оперативного керівництва у Збройних Силах України, незважаючи на значне розширення ринку інформаційних послуг і продуктів, а також певний розвиток законодавчої бази щодо інформатизації та інформаційного забезпечення залишається на низькому рівні.

Аналіз відомих досліджень та постановка задач. В наукових публікаціях, присвячених проблемам відмовостійкості [2-6] розглядається, що використання інформаційних ресурсів спрощує процес прийняття рішень на застосування сил і засобів, які повинні системно реагувати на інформаційні впливи та інформаційні загрози. Базова функціональність таких систем обробки інформації досягається на основі реалізації у їх підсистемах розвідки та інформаційного забезпечення принципів управління, а однією із найважливіших умов дієздатності є потреба оцінювання інформаційних ресурсів, які генерує кожна із них.

В [3] зазначається, що принципові завдання побудови автоматизованих систем управління виконувались для реалізації концепції мережецентричних війн за умови коли сили і засоби розвідки оцінили декілька відомостей та провели класифікацію за джерелами з яких отримані дані. Іншими словами, без актуальної інформації будь-яка автоматизована система не спроможна виконати функціональні завдання за призначенням.

У статті [4] визначено, що у сучасній моделі ведення збройної боротьби є ряд небезпечних недоліків пов'язаних з надмірним адмініструванням процесу інформаційного забезпечення автоматизованих систем управління військами (силами). Але за умов неповних відомостей та даних про противника при малоефективній автоматизованій системі управління військами (силами), виникає ситуація коли кожне рішення буде недостатньо обґрунтованим у зв'язку з відсутністю інтегральних функцій щодо механізму нарощування взаємодії з іншими інформаційними системами.

Проведений аналіз робіт [7-10] присвячених обґрунтуванню показників відмовостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України вказує на відсутність підходів, які дозволяють оцінювати шляхи надання відповідних протоколів обміну для забезпечення інформаційних систем логічною узгодженістю між іншими базами даних в існуючій автоматизованій системі управління військами (силами).

Зазначене вказує на необхідність обґрунтування показників відмовостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України, що обумовлено відсутністю переліку функцій, щодо забезпечення передачі даних між інформаційно-телекомунікаційними мережами основних та резервних автоматизованих систем управління військами (силами).

Метою статті є обґрунтування показників відмовостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України для подальшого визначення переліку функцій, що підлягають автоматизації за ступенем їх деталізації в системі управління військами (силами).

Основні результати досліджень. Основними проблемами центру оперативного керівництва Збройних Сил України вважаються застарілість або неефективне використання апаратного та програмного забезпечення, відсутність швидкісних захищених мереж передачі даних та централізованих сховищ даних, складність організації доступу до існуючих баз даних, відсутність єдиного формату обміну даними, і як наслідок – низька оперативність та недостовірність інформації.

Ефективне інформаційне забезпечення центру оперативного керівництва Збройних Сил України полягає у забезпеченні керівництва своєчасною та достовірною інформацією шляхом використання безперервних ІТ-сервісів.

Безперервність ІТ-сервісів є головною умовою, що застосовується при побудові центру оперативного керівництва Збройних Сил України, в який закладено комплекс заходів по забезпеченню постійної працездатності програмно-апаратних компонентів.

Це дозволяє зручно здійснювати планування та спрощує роботу користувачів по оформленню документів, що заощаджує час, але не може ефективно застосовуватися для забезпечення ситуаційної обізнаності під час ведення активних бойових дій. При розробці архітектури автоматизованої системи управління центру оперативного керівництва Збройних Сил України є потреба змістити акцент до ситуаційної обізнаності, як основи управління, а не резервування даних. Якщо переглянути архітектуру безперервності ІТ-сервісів, яка може розглядатись як сервіс на рівні оперативного командування або вище для резервування даних та планування ефективного використання, що в свою чергу задовольнить обрис вимог до автоматизованої системи управління центру оперативного керівництва Збройних Сил України.

Ключові характеристики, які визначають вимоги до безперервності ІТ-сервісів, наведені на (рис. 1).

Рисунок 1 – Цільова точка і цільовий час відновлення

На рис. 1 наведено зміст цільової точки відновлення та цільового часу відновлення для порівняння інтервалів часу в кожній із них.

RPO (*Recovery Point Objective*) – цільова точка відновлення – інтервал часу, що передує аварії, за який допускається втрата даних. Іншими словами, цей параметр показує, наскільки стан системи і даних може бути повернений назад при виникненні надзвичайної ситуації.

RTO (*Recovery Time Objective*) – цільовий час відновлення – інтервал часу після аварії, необхідний для відновлення стану системи і даних.

Відповідно, RTO показує час допустимого простою, а RPO – обсяг втрати даних. Теоретично значення RTO/RPO = 0 є найкращим: простій і втрата даних неприпустимі.

На практиці, досягнути RTO = 0 можливо у дуже обмеженому числі випадків, наприклад, коли можливе дублювання функціонально ідентичних апаратних компонент (блоків живлення, дисків, контролерів дискових масивів, мережевих портів).

У випадку більш масштабних аварій (наприклад, відмови серверу або системи) досягнути показника нульового RTO або неможливо фізично, або це може призвести до неприйнятного подорожчання чи ускладнення системи.

З цієї причини, на практиці під нульовим RTO доцільно розуміти час простою, що лежить в межах так званої еластичності функціональних процесів, що виражається в часових одиницях. Величина цієї еластичності може коливатися від декількох десятків секунд до декількох годин (табл. 1).

Таблиця 1

Типові значення часової затримки функціональних процесів

Функціональний процес	**Типова тривалість затримки**
Системи масового обслуговування	10-30 сек.
АРМ оператора оперативного управління	1-5 хв.
АРМ оператора забезпечення (логістика)	15-30 хв.
АРМ адміністративних процесів (персонал)	1-2 год.

Першим з кроків у проектуванні комплексу організаційно-технічних заходів, спрямованих на недопущення затримки, є визначення моделі загроз безперервності ІТ-сервісів і цільових параметрів RTO/RPO реагування на них. Типова модель загроз представлена в табл. 2.

Таблиця 2

Модель загроз безперервності надання ІТ-сервісів

Класи загрози	**Опис**	**Частота**	**Типові засоби захисту**
А1. Локальні відмови	Некратні відмови устаткування та ПЗ, що призводять до непрацездатності однієї або декількох операційних систем.	Часто, до декількох разів на місяць.	Дублювання апаратних компонентів, холодний резерв, кластери, функції ОС центру оперативного керівництва (шар віртуалізації)
А2. Локальні катастрофи	Непрацездатність центру оперативного керівництва. Типові причини – відмова системи електроживлення або охолодження, локальна пожежа	Дуже рідко. Один раз в 3-5 років	Синхронний симетричний або асиметричний резервний центр оперативного керівництва (<50 км)
А3. Регіональні катастрофи	Одночасна непрацездатність всіх центру оперативного керівництва на відстані до 100 км. типові причини – масштабні порушення в роботі систем енергопостачання, повені, масові заворушення	Вкрай рідко. Один раз на/за кілька десятиліть	Асинхронний асиметричний резервний центр оперативного керівництва (>100км)

B1. Руйнування даних на рівні логіки	Порушення логічної цілісності даних , викликане збоями ПЗ або помилками людини	Рідко. Кілька разів на рік	Система резервного копіювання і відновлення
B2. Вікно обслуговування	необхідність тимчасової зупинки IT-сервісів для проведення регламентного обслуговування устаткування і ПЗ	Часто. До декількох разів на місяць.	Мобільність робочих навантажень
B3. Зміни	Внесення змін в інфраструктуру або програмний ландшафт (модернізація обладнання, оновлення ПЗ, міграція центру оперативного керівництва, впровадження нових IT-сервісів)	Часто. До декількох разів на місяць.	Процес управління змінами кошти на попереднє тестування змін
B4. Складність	Мимовільна дестабілізація складних систем (наприклад, багатовузлових географічно розподілених кластерів) як результат непередбачуваного збігу обставин або викликані цією складністю помилки адміністрування	Рідко. Кілька разів на рік	Спрощення архітектури, автоматизація сценаріїв адміністрування

Аналіз результатів табл.1 показує, що із класу загроз найбільш розповсюдженими є локальні відмови, що призводять до непрацездатності однієї або кількох операційних систем декілька разів на рік. Що в порівнянні із руйнуванням даних на рівні логіки дозволяє системі самій адмініструвати копіювання і відновлюватись.

Тому показники відмовостійкості цільової точки відновлення та цільового часу відновлення RTO/RPO автоматизованої системи управління центру оперативного керівництва Збройних Сил України повинні мати оціночні характеристики, як для врахування самостійного, так і регламентного відновлення.

До основних показників регламентного відновлення відносяться:

резервне копіювання та архівування даних на віддаленому сервері (*Crossite backup*) з розміщенням їх;

різні способи реплікації даних на віддалену платформу з розміщенням їх на дискових масивах.

Наведені показники регламентного відновлення дозволяють прогнозувати сценарії можливих локальних і, тим більше, регіональних катастроф, які відрізняються від локальних відмов значно більшою масштабністю і варіативністю. На практиці неможливо передбачити всі можливі варіанти розвитку катастроф, які саме підсистеми IT-інфраструктури будуть

порушені і в якому порядку. З цієї причини реакція на катастрофу повинна визначатися чітким сценарієм дій, змістом і послідовністю враховуючи особливості конкретної ситуації.

Такий сценарій носить назву *DR-плану* (план відновлення у випадку фізичного знищення автоматизованої системи управління центру оперативного керівництва Збройних Сил України).

Типовий DR-план автоматизованої системи управління центру оперативного керівництва Збройних Сил України може включати в себе десятки і сотні послідовних і паралельних кроків щодо порядку залучення людських та технічних ресурсів. Кожен технічний або організаційний механізм захисту повинен бути приведений у дію відповідно до загального сценарію відновлення, з урахуванням конкретної ситуації і взаємодії з іншими механізмами. Одночасне спрацьовування великої кількості окремих механізмів захисту (як автоматизованих, так і ручних) без жорсткого регулювання, на практиці може призводити до взаємно деструктивних і блокуючих наслідків, у результаті чого вся система буде недієздатна.

Таким чином, адекватна реакція на катастрофічні події без DR-плану автоматизованої системи управління центру оперативного керівництва Збройних Сил України неможлива. Водночас, велика варіативність катастроф призводить до того, що неможливо створити універсальний DR-план автоматизованої системи управління центру оперативного керівництва Збройних Сил України, який би враховував всі можливі сценарії розвитку подій.

Виконання DR-плану автоматизованої системи управління центру оперативного керівництва Збройних Сил України завжди проводиться в контексті конкретної ситуації і особливості цієї ситуації, що напряму впливає на відповідні дії і їх послідовність, при виконанні DR-плану. На даному етапі розвитку технологій лише людина здатна на подібну корекцію і деталізацію DR-плану в реальному часі. Це означає, що виконання DR-плану центру оперативного керівництва Збройних Сил України без контролю людини неможливо. Водночас, необхідність участі людини у виконанні DR-плану центру оперативного керівництва Збройних Сил України не означає, що DR-план не піддається автоматизації. Навпаки, автоматизація є ефективною для рутинних "*атомарних*" процедур, які є складовими DR-плану центру оперативного керівництва Збройних Сил України.

Подібна автоматизація дозволяє людині сконцентруватися виключно на своїх функціях: загальній оцінці ситуації та прийнятті рішення про приведення в дію DR-плану центру оперативного керівництва Збройних Сил України та контроль за його виконанням, внесенням коригувань до послідовності дій при нештатних ситуаціях, взаємодії з іншими посадовими особами або організаціями.

IT-інфраструктура автоматизованої системи управління центру оперативного керівництва Збройних Сил України постійно піддається змінам. З цієї причини DR-план може з часом втрачати свою актуальність. Для цього його необхідно постійно уточнювати та періодично тестувати.

Основною проблемою при тестуванні DR-плану як елементу системи відмовостійкості центру оперативного керівництва Збройних Сил України є вплив на роботу продуктивних систем, що призводить до появи нових загроз безперервності IT. Виникає протиріччя, коли DR-план (а саме – необхідність його тестування), призначений для забезпечення безперервності IT, сам може стати загрозою для безперервності функціонування серверів.

З цієї причини максимальна ізоляція продуктивного і резервного дублювання, особливо на період тестування DR-плану центру оперативного керівництва Збройних Сил України, стає ключовою архітектурною вимогою. Ці вимоги потребують проведення аналізу інформаційних загроз відповідно до умов інформаційної технології які наведені в (табл. 2).

Наведені характеристики DR-плану центру оперативного керівництва Збройних Сил України дають можливість запропонувати для кожного класу загроз показники

відмовостійкості, як перелік функцій, що підлягають автоматизації за ступенем їх деталізації в системі управління військами (силами).

А1. Локальні відмови. Оптимальний метод захисту – автоматизовані засоби локальної відмовостійкості.

Дотримуючись принципу "*одне завдання - одне рішення*" доцільним є реалізація механізмів відмовостійкості на рівні рішення віртуалізації та автоматизації . Водночас, це не виключає використання обмеженої кількості специфічних для прикладного ПЗ засобів.

А2. Локальні катастрофи. Оптимальний метод захисту – синхронний резервний центр із частково автоматизованим DR-планом системи управління центру оперативного керівництва Збройних Сил України.

Основні і резервні функції, які підлягають автоматизації в центрі оперативного керівництва Збройних Сил України можуть бути застосовані в режимі "*активний-активний*", тобто кожен з них може нести корисне навантаження. При втраті одного з центрів з метою виключення деградації продуктивності DR-план повинен передбачати зупинку допоміжних додатків (наприклад, процесів розробки) і вивільнення додаткових ресурсів для продуктивного серверу системи. Повинні бути передбачені витрати на періодичне тестування DR-плану з мінімальним (нульовим) впливом на продуктивний сервер.

А3. Регіональні катастрофи. Оптимальний метод захисту – асинхронна або резервна автоматизована система управління центру оперативного керівництва Збройних Сил України. Асинхронна автоматизована система управління центру оперативного керівництва Збройних Сил України може бути асиметричною, тобто містити ресурси, необхідні тільки для зберігання баз даних і запуску на їх основі найбільш критичних масивів. Активація асинхронної автоматизованої системи управління центру оперативного керівництва Збройних Сил України дозволяє застосувати показники відмовостійкості цільової точки відновлення та цільового часу відновлення RTO/RPO, які необхідні для повернення до використання основної автоматизована система управління центру оперативного керівництва Збройних Сил України.

В1. Логічне руйнування даних. Оптимальний метод захисту – система резервного копіювання або відновлення. Слідуючи принципу "*одне завдання - одне рішення*" доцільним є реалізація механізмів резервного копіювання та відновлення на рівні операційних систем автоматизованої системи управління центру оперативного керівництва Збройних Сил України. Обов'язковим елементом системи повинна бути процедура періодичної перевірки можливості відновлення прикладних процесів з використанням резервної копії даних.

В2-В4. Обслуговування, зміни, складність. Оптимальними методами захисту – є мобільність робочих навантажень, процес управління змінами (включаючи інструменти попереднього тестування наслідків змін без впливу на продуктивний сервер системи), усунення зайвої складності або невиправданого автоматизму спрацьовування засобів захисту.

Аналіз наведених функцій показує, що кожна з них має певні особливості, реагування на які потребує впровадження на ряду з показниками відмовостійкості цільової точки відновлення та цільового часу відновлення RTO/RPO такого, як безперервності ІТ-сервісів автоматизованої системи управління центру оперативного керівництва Збройних Сил України.

Врахування додаткового показника відмовостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України, зокрема безперервності ІТ-сервісів є необхідним, оскільки ІТ-інфраструктура автоматизованої системи управління залежить від технологій, які постійно удосконалюються та має відповідати вимогам:

захист від витоку інформації під час передачі її між основною та резервною автоматизованою системою управління центру оперативного керівництва Збройних Сил України;

можливість забезпечення взаємодії з існуючими автоматизованими системами, що функціонують в Збройних Силах України;

можливість взаємодії з інформаційними системами країн членів НАТО.

Реалізація наведених вимог буде можлива шляхом виконання запропонованого узагальненого алгоритму перевірки існуючої системи забезпечення безперервності ІТ-сервісів.

1. Забезпечення безперервності ІТ-сервісів:

захист ІТ-сервісів від загроз;

визначення найбільш важливих ІТ-сервісів за ступенем критичності на основі результатів аналізу взаємозалежностей ІТ-сервісів та їх впливу на функціональні-процеси;

визначення цільових RTO/RPO.

2. DR-план – розробка, оновлення і перевірка:

підготовка плану відновлення;

перевірка актуальності плану відновлення;

проведення тестової перевірки плану відновлення;

приведення до вимог автоматизованим DR-планом системи управління центру оперативного керівництва Збройних Сил України.

3. Підготовка персоналу до виконання DR-плану:

проведення періодичних тренувань по виконанню вимог автоматизованим DR-планом системи управління центру оперативного керівництва Збройних Сил України;

визначення залікового рівня підготовки персоналу.

4. Проведення тестової активації та передачі управління до резервної автоматизованої системи управління центру оперативного керівництва Збройних Сил України:

перевірка готовності резервної автоматизованої системи управління центру оперативного керівництва до активації;

перевірка суміжності в роботі резервної і основної автоматизованої системи управління центру оперативного керівництва.

5. Перевірка придатності резервних копій даних для відновлення ІТ-сервісів:

перевірка можливості фізичного зчитування резервних копій з носіїв;

тестова перевірка когерентності цих копій;

перевірка можливості відновлення ІТ-сервісів на випадок пошкодження даних;

проведення тестування придатності резервних копій для відновлення прикладних систем забезпечення безперервності ІТ-сервісів.

Врахування наведеного узагальненого алгоритму перевірки існуючої системи забезпечення безперервності ІТ-сервісів під час визначення показників відмово стійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України дозволить організувати безперебійну роботу критичних ІТ-систем в новітній Єдиній автоматизованій системі управління військами (силами).

Зазначене потребує в життєвому циклі функціонування автоматизованої системи управління центру оперативного керівництва Збройних Сил України розглядати технологічну та економічну складові. Технологічна з’являється на стадіях проектування та будівництва шляхом врахування цільової точки відновлення ІТ-сервісів.

З фінансової точки зору життєвий цикл створення та функціонування центру оперативного керівництва Збройних Сил України характеризується зростанням капітальних витрат, пік яких припадає на першу половину стадії будівництва, з виходом в рівноважну точку досягненні граничного терміну експлуатації коли вартість підтримання об’єкта в належному стані не виправдовується його цільове призначення. Ці умови потребують

проведення фінансових розрахунків щодо визначення сукупної вартості володіння (*Total cost of ownership – TCO*).

ТСО – є ключовим кількісним показником ефективності процесів автоматизації, який дозволяє оцінити сукупні витрати на інформаційні технології (обладнання, інструментальні засоби, процеси супроводу інформаційних систем, а також дії кінцевих користувачів), аналізувати їх і відповідно управляти витратами (бюджетом) для досягнення балансу доцільності та вартості прямих витрат.

Розрахунок прямих витрат під час створення та функціонування центру оперативного керівництва Збройних Сил України включає як обладнання його амортизацію, так і адміністрування інфраструктури, введення обладнання в експлуатацію, електрика, оплата праці працівників і послуг підрядників, навчання, зв'язок) в ТСО враховуються і непрямі витрати:

втрати від планових і позапланових збоїв в роботі обладнання та ПЗ;

втрати часу співробітників на самостійне управління користувацькими пристроями і додатками;

порушення інформаційної безпеки.

Ключовим принципом створення та функціонування центру оперативного керівництва Збройних Сил України, є системний підхід, який дозволяє оцінити вартість майбутньої та дає уявлення про ймовірні втрати в процесі експлуатації. Незважаючи на те, що більшість витрат можуть бути передбачені або спрогнозовані з високою точністю, деякі витрати носять імовірнісний характер, що тягне за собою ризик істотних відхилень дійсних витрат від очікуваних.

Висновки. Основою інтеграції існуючих та перспективних інформаційних систем є центри оперативного керівництва Збройних Сил України, які поєднані у єдиний інформаційний простір та створюють єдине інформаційне середовище з інтегрованою базою даних та єдиними сервісами обміну базами даних. Врахування запропонованого переліку функцій, які підлягають автоматизації за ступенем їх деталізації в системі управління військами (силами) дозволить здійснювати резервування передачі даних між інформаційно-телекомунікаційними мережами основних та резервних автоматизованих систем управління центрами оперативного керівництва Збройних Сил України. Врахування доцільних показників відмовостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України, якими є цільова точка відновлення та цільовий час відновлення RTO/RPO підвищить оперативність функціональних процесів в кризових ситуаціях під час застосування конкретної моделі загроз безперервності надання ІТ-сервісів. Особливе місце в процесі відмовостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України займає показник безперервності ІТ-сервісів. Тому, що врахування його характеристик дозволить удосконалювати ІТ-інфраструктуру автоматизованої системи управління, що є фундаментом єдиного інформаційного середовища Збройних Сил України. Впровадження показників, які характеризують фінансові розрахунки щодо визначення сукупної вартості створення та функціонування центру оперативного керівництва Збройних Сил України забезпечить додаткове прогнозування витрат на розвиток Єдиної автоматизованої системи управління військами (силами).

ЛІТЕРАТУРА:

1. Звіт Департаменту внутрішнього аудиту Міністерства оборони України № 234/4341 від 18.12.2020 [Електронний ресурс]: bihus.info. – Режим доступу: http://bihus.info/vijskovi-zlyly-600-mln-na-systemu-upravlinnya-armiyeyu-yaka-mozhe-vyyavytysya-vzagali-neprydatnoyu.

2. Про Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України [Електронний ресурс]: указ [видано Президентом України 14 квітня 1999 р. № 379/99]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/379/99.

3. Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2015 року [Електронний ресурс]: постанова [видано Кабінетом Міністрів України 7 вересня 2011 р. № 942-2011-п (Із змінами)]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/942-2011-%D0%BF.

4. Уряд планує створити ситуаційний центр [Електронний ресурс]. – Режим доступу: http://defpol.org.ua/site/index.php/ru/arhiv/2010-01-06-09-33-10/8713-2012-02-08-12-24-20.

5. Коммерческие ЦОД в Украине: новый этап развития [Электронный ресурс]. – Режим доступа: http://www.sib.com.ua/arhiv_2010/2010_3/ statia_3_1_2010/statia_3_1_2010.htm.

6. Institute for Data Center Professionals [Electronic Resource]. – Mode of access: http://idcp.marist.edu.

7. Uptime Institute LLC [Electronic Resource]. – Mode of access: http://uptimeinstitute.com.

8. TIA/EIA-942. Telecommunications Infrastructure Standard for Data Centers. – SP–3-0092, 2005. – 151 p.

9. EN 50173-5. Information technology – Generic Cabling Systems – Part 5: Data Centres. – European Standards(EN), 2007. – 140 p.

10. Датацентр консалтинг: Denovo [Электронный ресурс]. – Режим доступа: http://www.de-novo.biz/chastnye-oblaka-i-korporativnye-tsody/datatsentr-konsalting.

REFERENCES:

1. Report of the Department of Internal Audit of the Ministry of Defense of Ukraine No. 234/4341 dated 18.12.2020 [Electronic resource]: bihus.info. – Access mode: http://bihus.info/vijskovi-zlyly-600-mln-na-systemu-upravlinnya-armiyeyu-yaka-mozhe-vyyavytysya-vzagali-neprydatnoyu.

2. About the Regulation on the Anti-Terrorist Center and its coordination groups under the regional bodies of the Security Service of Ukraine [Electronic resource]: decree [issued by the President of Ukraine on 14 April 1999 p. № 379/99]. – Access mode: http://zakon2.rada.gov.ua/laws/show/379/99.

3. On approval of the list of priority thematic areas of scientific research and scientific and technical development for the period until 2015 [Electronic resource]: resolution [issued by the Cabinet of Ministers of Ukraine on September 7, 2011 № 942-2011-п]. – Access mode: http://zakon4.rada.gov.ua/laws/show/942-2011-%D0%BF.

4. The government plans to create a situation center [Electronic resource]. – Access mode: http://defpol.org.ua/site/index.php/ru/arhiv/2010-01-06-09-33-10/8713-2012-02-08-12-24-20.

5. Commercial data center in Ukraine: new stage of development [Electronic resource]. – Access mode: http://www.sib.com.ua/arhiv_2010/2010_3/ statia_3_1_2010/statia_3_1_2010.htm.

6. Institute for Data Center Professionals [Electronic Resource]. – Mode of access: http://idcp.marist.edu.

7. Uptime Institute LLC [Electronic Resource]. – Mode of access: http://uptimeinstitute.com.

8. TIA/EIA-942. Telecommunications Infrastructure Standard for Data Centers. – SP–3-0092, 2005. – 151 p.

9. EN 50173-5. Information technology – Generic Cabling Systems – Part 5: Data Centres. – European Standards(EN), 2007. – 140 p.

10. Data center consulting: Denovo [Electronic Resource]. – Electronic Resource: http://www.de-novo.biz/chastnye-oblaka-i-korporativnye-tsody/datatsentr-konsalting.

PhD Katsalap V.O.,
Omelianchuk A.V,.
Syvak O.V.

JUSTIFICATION OF INDICATORS OF FAILURE RESISTANCE OF THE AUTOMATED CONTROL SYSTEM OF THE CENTER OF OPERATIONAL MANAGEMENT OF THE ARMED FORCES OF UKRAINE

Modern approaches to substantiating the failure-tolerance indicators of the automated control system of the operational command center of the Armed Forces of Ukraine are based on the fact that any process of accumulating, collecting and storing information is invariably cyclic in nature. This essence determines the need to justify the indicators that allow data to be backed up in the automated management system. Such indicators of fault tolerance of the automated control system of the operational management center include: target recovery point - RPO; target recovery time - RTO; continuity of IT-services. The given indicators determine the effectiveness of the information support of the automated management system, which consists in providing management with timely and reliable information.

This is especially relevant in the conditions of full-scale armed aggression of the Russian Federation against Ukraine and requires improvement of approaches to ensure the resilience of the automated control system of the operational command center of the Armed Forces of Ukraine.

The model of IT-service continuity threats developed in the article makes it possible to compare classes of threats with their frequency of occurrence and typical means of protection. Based on them, it is possible to compare the corresponding indicators of scheduled recovery, in particular backup and archiving of data on a remote server (Crossite backup).

In addition, the work considers approaches based on the application of financial indicators of the effectiveness of automation processes (Total cost of ownership), which allow to estimate the total costs of information technologies (equipment, tools, processes of supporting information systems.

Keywords: center, operational management, special software, fault tolerance, automated control system, automated information systems, Armed Forces of Ukraine.