DOI: **10.33099/2311-7249/2022-48-3-98-106**

УДК 681.5; 654.9

Панченко Сергій Миколайович [1]
Антонюк Андрій Георгійович [2]
Новицький Дмитро Владиславович [1]
Усок Сергій Олександрович [2]
Заморський Сергій Миколайович [2]

[1] ***Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна***
[2] ***Головне управління зв'язку та кібербезпеки Генерального Штабу Збройних Сил України, Київ, Україна***

ЗАГАЛЬНІ ПІДХОДИ ДО СТВОРЕННЯ СИСТЕМИ УПРАВЛІННЯ І КОНТРОЛЮ ФУНКЦІОНУВАННЯ СЕРВІСІВ ІНФОРМАЦІЙНИХ СИСТЕМ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Актуальність тематики викладеного матеріалу обґрунтовується рівнем сучасного розвитку системи управління Збройними Силами України та її матеріально-технічної основи – системи зв'язку, яка, в свою чергу, вже давно вийшла за межі вимог щодо забезпечення суто зв'язку. Метою статті є формування єдиних підходів до використання сервісів з управління і контролю інформаційних систем в сервіс-орієнтованому середовищі системи зв'язку та інформаційних систем Збройних Сил України, а також створення підґрунтя для впровадження архітектурного планування інформаційних технологій у Збройних Силах України. Під час написання статті застосовано такі методи досліджень як системний аналіз та структурний синтез. Зазначений методичний підхід дає змогу провести аналіз функціонування інформаційних сервісів та визначити вимоги до них щодо управління і контролю. Акцентовано увагу, що керівними документами стосовно створення та впровадження інформаційних систем є Закони України, Постанови Кабінету Міністрів України, накази та розпорядження Міністерства оборони України, Головнокомандувача Збройних Сил України, начальника Генерального штабу Збройних Сил України, інші нормативно-правові документи у різних сферах діяльності. Для досягнення паритету перед ворогом у часовому циклі прийняття рішення, підвищення ефективності застосування озброєння і військової техніки та отримання інформаційної переваги під час прийняття рішень в процесі управління військами, у Збройних Силах України продовжують впроваджуватися та нарощуватися різноманітні інформаційні системи. Сервіси інформаційних систем широко використовуються службовими особами Збройних Сил України у власній діяльності. Мета їх застосування полягає в автоматизації (цифровізації) функціональних процесів у Збройних Силах України та досягненні ефективних (бажаних) результатів, цілей за найменш короткий проміжок часу з максимально можливою ефективністю. У статті сформульовані загальні підходи щодо створення системи управління і контролю функціонування сервісів інформаційних систем у Збройних Силах України, що ґрунтуються на досвіді застосування військових частин (підрозділів), а також відповідають кращим світовим практикам використання інформаційних технологій. Наведено необхідний понятійний апарат щодо існування сервісів інформаційних систем. У статті наведена функціональна модель системи управління та контролю функціонування сервісів, яка запроваджує систему інформаційних зв'язків між функціональними модулями та визначає зміст технологічної інформації, що циркулюватиме в ній. Практичною реалізацією положень статті є те, що запропонована модель дає змогу сформувати та стандартизувати підходи до побудови системи управління і контролю функціонування сервісів інформаційних систем, які застосовуються з метою автоматизації (цифровізації) процесів управління в Збройних Силах України. Напрямом подальших досліджень є розроблення методичного апарату оцінювання ефективності функціонування системи управління і контролю функціонування сервісів інформаційних систем різного призначення.

Ключові слова: *інформаційні технології, система зв'язку, інформаційні системи, інформаційні сервіси, сервіси з управління і контролю інформаційних систем.*

Вступ

Збройні Сили України (далі – ЗС України) у своїй діяльності широко використовують інформаційні технології (далі – ІТ), що забезпечують базові та функціональні послуги (сервіси) автоматизованих та інформаційних систем, систем забезпечення ситуаційної обізнаності, а також систем підтримки прийняття рішень. Їх стрімке поширення зумовлене необхідністю адаптації до сучасності, бути кращими та ефективнішими за ворогів, які ведуть підступну загарбницьку війну проти України в умовах постійної обмеженості у людських та матеріальних ресурсах. Сучасні глобальні ІТ дають змогу будувати якісні функціональні рішення на користь ЗС України. Водночас з'явилася велика

кількість програмно-апаратних рішень (засобів, комплексів, систем), використання яких обумовлене надзвичайно складними завданнями, що потрібно виконувати силами оборони держави. Варіанти реалізації зазначених рішень настільки різноманітні в ІТ-додатках, що процеси їх розгортання та впровадження вже потребують архітектурного узгодження, стандартизації методів, оскільки вони вступають у дію (виконують завдання) і вимагають від ЗС України виділення потрібних ресурсів. Тому, розвиток ІТ-напряму у ЗС України потребує концептуальних документів, для забезпечення власного функціонування з урахуванням актуальних перспектив і сучасних тенденцій у розвитку ІТ-індустрії.

Постановка проблеми. Проблемою, з якою зараз стикаються ЗС України, є складність розуміння існуючих можливостей застосування сучасних методів (на підставі кращих світових ІТ-практик), які забезпечують існування життєвого циклу сервісів (служб, послуг) інформаційних систем. Сьогодні трактування різних інформаційно-технологічних понять, методів і технічної термінології у ЗС України не уніфіковано або не відповідає сучасним вимогам. Це негативно впливає на якість роботи існуючих інформаційних та автоматизованих систем, впровадження нових сервісів і виведення старих з експлуатації, що також призводить до інерції, труднощів у розвитку та розширенні переліку сервісів, недостатніх або непередбачуваних витрат ресурсів, проблем в управлінні персоналом, а також появи корупційних ризиків.

Аналіз остатніх досліджень і публікацій. Під час впровадження (створення) різних систем (автоматизованих, інформаційних, ситуаційної обізнаності тощо) використовуються державні та міжнародні стандарти [1, 4-6], Закони України [2], постанови Кабінету Міністрів України [3], доктринальні документи, методичні рекомендації (настанови, інструкції) та інші документи (накази та розпорядження), які затверджені керівниками (начальниками) відповідних відомств (підрозділів, установ та організацій), що підпорядковані Міністерству оборони України, Головнокомандувачу Збройних Сил України та начальнику Генерального штабу Збройних Сил України. Серед останніх, найбільш прийнятною та обґрунтованою військовою публікацією залишається Доктрина «Зв'язок та інформаційні системи» [7]. Зазначений документ, який був затверджений Головнокомандувачем ЗС України у липні 2020 року, визначає загальне керівництво і застосування зв'язку та інформаційних систем у ЗС України й інших складових сил оборони [7]. Доктрина вводить термінологію в галузі комунікаційних та інформаційних систем, що сумісна з термінологією, прийнятою в країнах – членах НАТО, описує характеристики цих систем, концепції управління інформацією, архітектуру побудови комунікаційних та інформаційних систем, захист інформації та захист мережі в інформаційно-комунікаційних системах. Водночас стрімкий розвиток і застосування інформаційних систем у ЗС України висуває нові вимоги до спільної роботи цих систем та забезпечення підтримки прийняття рішень органами військового управління. Тому актуальними постають питання управління і контролю функціонування сервісів інформаційних систем.

Метою статті є формування єдиних підходів до використання сервісів з управління і контролю інформаційних систем в сервіс-орієнтованому середовищі системи зв'язку та інформаційних систем Збройних Сил України, а також створення підґрунтя для впровадження архітектурного планування ІТ у ЗС України.

Виклад основного матеріалу дослідження

Під поняттям *"управління та контроль сервісами інформаційної системи"* пропонується розуміти діяльність, що характеризується набором взаємопов'язаних політик (правил) для реалізації визначених функціональних процесів, серед яких визначаються ролі та відповідальність, а також визначаються інструменти для використання цих процесів.

Для подальшого викладення матеріалу необхідно визначити понятійний апарат, який дозволяє зрозуміти основні взаємопов'язані функціональні процеси, необхідні для існування сервісів інформаційної системи.

Формування цінностей, спроможностей та відповідальностей – є процесами їх визначення (встановлення), створення (розробки) необхідних функціональних алгоритмів, побудови порядку інформаційних взаємодій, визначення спроможностей користувачів та порядку їх набуття, визначення порядку розробки сервісу інформаційних систем, впровадження, супроводження функціонування, масштабування, модернізації та виведення з експлуатації, а також визначення відповідальності осіб для забезпечення сталого функціонування сервісів інформаційних систем.

Формування інфраструктури (інфраструктурні) – процеси побудови необхідної інфраструктури для функціонування сервісів інформаційних систем, побудова спеціально обладнаних технічних майданчиків (автоматизованих робочих місць), включно із системами контролю доступу, відеоспостереження, електрозабезпечення, кліматичними системами, резервними та рухомими об'єктами, апаратними, програмними, програмно-апаратними компонентами, технологіями та даними, що формуються, висвітлюються, зберігаються та обробляються, інформаційно-аналітичними, експертними системами.

Організаційно-технічні (адміністративні) процеси – це процеси реалізації заздалегідь спланованих рішень, спрямованих на забезпечення сталого функціонування сервісів інформаційних систем, що розкривають питання організації роботи технічного персоналу.

Користувальницькі процеси – регламентують (охоплюють) діяльність всіх користувачів сервісів інформаційних систем.

Стійке функціонування сервісів інформаційної системи забезпечується за допомогою функціональних засобів (інструментів або сервісів управління та контролю), реалізація яких покладається на технічний персонал. Тому саме технічний персонал супроводжує функціонування сервісів інформаційних систем, розгортає та використовує перелік визначених сервісів. Загалом, на технічний персонал покладаються такі завдання:

сервіс контролю за технічною інфраструктурою;

сервіс контролю за інфраструктурою центрів обробки даних (далі – ЦОД), (хмарних обчислень);

сервіс з управління (адміністрування);

сервіс моніторингу;

сервіс вимірювання;

сервіс протоколювання;

сервіс технічної підтримки;

сервіс інформаційно-аналітичних систем;

сервіс експертних систем кіберзахисту.

Використання вищезазначених сервісів дає змогу відстежувати поточний стан роботи сервісів інформаційної системи, їх доступність для користувачів, фіксувати їхню діяльність, виявляти можливі порушення в роботі, що може бути пов'язано з відхиленнями елементів роботи від стандартів.

Водночас, користування означеними сервісами забезпечить швидку реакцію на інциденти, розробку і застосування запобіжних заходів щодо можливих майбутніх інцидентів у роботі, вияв і нівелювання мережевих кібервпливів, вимірювання, аналіз й прогнозування продуктивності та ефективності використання і витрачання необхідних ресурсів.

У свою чергу, на персонал, який забезпечує управління і контроль покладаються такі завдання:

контроль за функціонуванням технічної інфраструктури – дає змогу контролювати умови функціонування технічного майданчика;

контроль за інфраструктурою ЦОД – дає змогу здійснювати контроль за функціонуванням систем віртуалізації, спостерігати за обчислювальними ресурсами, контролювати міграцію та резервування необхідних даних;

управління (адміністрування) сервісами інформаційних систем, означає спроможність технічного персоналу здійснювати їх розгортання, відновлення, конфігурування, зберігання та резервування необхідних даних;

моніторинг дає змогу здійснювати контроль за функціонуванням та доступністю сервісів інформаційних систем в інтересах користувачів на постійній основі, здійснювати аналіз мережевого трафіку комунікаційних сервісів;

протоколювання функціонування сервісів інформаційних систем, дає змогу налагоджувати процеси з формування технологічних даних, їх передачу/отримання, зосередження, підготовку цих даних для аналізу та передачі їх до систем відображення;

технічна підтримка збереження та архівування даних про функціонування;

інформаційно-аналітичні системи виявлення аномальної (нестандартної) поведінки внутрішніх процесів;

експертні системи кіберзахисту дають змогу вчасно реагувати на інциденти та кібервплив; запобігати відмовам у роботі; вимірювати функціональні показники, здійснювати їх аналіз і прогнозування роботи інформаційних систем і сервісів. На основі отриманих аналітичних даних ці системи дозволяють ефективно розподіляти, використовувати ресурси, заощаджувати та оцінювати відповідність сервісів інформаційних систем встановленим меті й завданням (цінностям).

Функціональна модель системи управління і контролю функціонування сервісів, з урахуванням інформаційних напрямів, наведена на рис. 1, складається з елементів що, забезпечують генерацію та структурованість інформації, потрібної для функціонування системи в цілому:

1. Формування і передача технологічних даних про функціонування інженерної інфраструктури технічних майданчиків.

2. Формування і передача технологічних даних від систем віртуалізації, резервування, комунікаційних сервісів і сервісів інформаційних систем до функціонального серверу збору технологічних даних про поточний стан функціонування.

3. Приймання, збір, обробка технологічних даних від джерел їх формування та подання у вигляді спеціалізованого технічного контенту, зрозумілого для технічного персоналу.

4. Зберігання та архівування технологічних даних.

5. Аналіз даних. Функціональна складова вирішує питання аналізу технологічних даних. Інформаційно-аналітичні системи здійснюють вимірювання та проведення розрахунків. Експертні системи кіберзахисту виконують завдання з пошуку та виявлення вразливостей.

6. Управління (адміністрування), технічна підтримка.

7. Відображення технологічної інформації. Для реалізації цієї функціональної складової розгортається комплекс технічних засобів відображення інформації, який призначений для подання технологічних даних у графічному або текстуальному вигляді. Мета – забезпечити максимальну зручність і функціональність подачі технологічної інформації в інтересах технічного персоналу для контролю та оперативного реагування на зміни у функціонуванні сервісів інформаційних систем.

З метою визначення ефективності функціонування системи пропонується сформулювати такі *вимоги до сервісів з управління і контролю.*

Технологічність – спроможність бути ефективними при використанні різного роду інформаційних технологій, апаратних рішень та не залежати лише від конкретних технологій.

Сучасність – спроможність впроваджувати, реалізовувати кращі сучасні практики функціонального напряму.

Гнучкість, адаптивність – спроможність швидко конструктивно змінюватися, адаптуватися під нові сформовані вимоги функціонування.

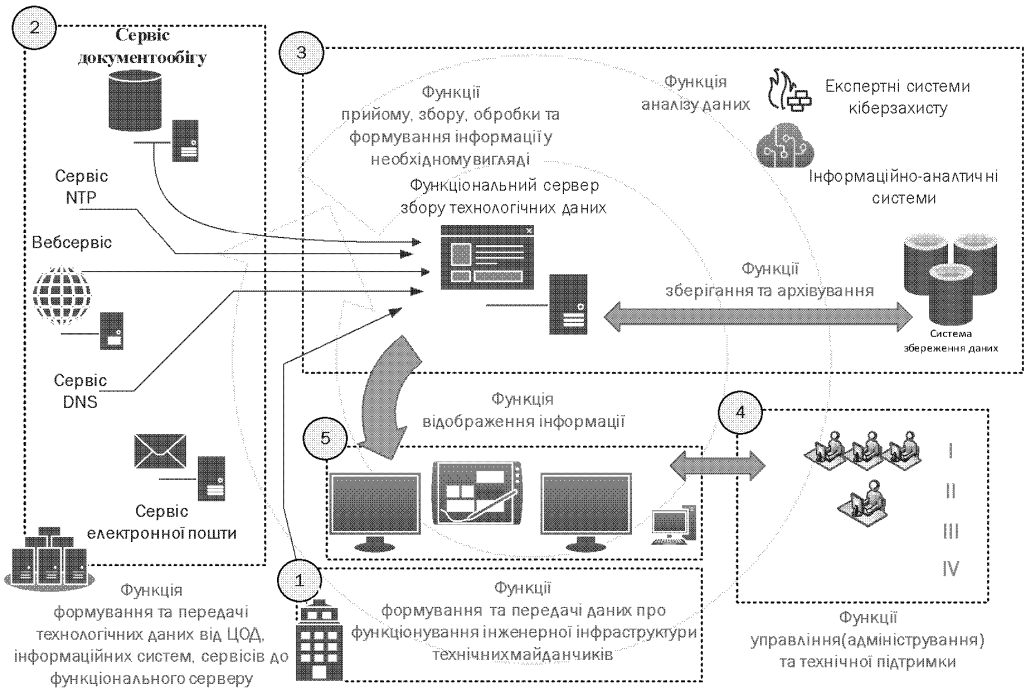

Рисунок 1 – Функціональна модель системи управління і контролю функціонування сервісів

Захищеність – спроможність протистояти зовнішньому та внутрішньому впливу.

Відмовостійкість – спроможність працювати відмовостійко та швидко відновлюватися.

Інформативність – спроможність представляти технологічну інформацію в простому, зрозумілому для технічного персоналу вигляді та мати глибоке кореневе взаємопов'язане аналітичне підґрунтя.

Легкість у використанні – спроможність бути легкою, нескладною.

Масштабованість – спроможність нарощувати свої кількісні, або якісні характеристики.

Аналітичність – спроможність здійснювати оцінку статистичних даних та прогнозувати майбутній стан об'єкта аналізу.

Ієрархічність – спроможність видавати технологічні дані за ієрархією адміністративності.

Структурованість – спроможність бути структурно прозорим, зрозумілим.

З урахуванням наведених вище вимог, усі без винятку сервіси інформаційних систем ЗС України в обов'язковому порядку повинні бути контрольованими за встановленими показниками функціонування. Показники функціонування сервісів інформаційних систем – це функціональні показники, за якими оцінюється їх поточний стан роботи або їх аномальна поведінка.

За результатами авторського аналізу використання інформаційних сервісів та визначення умов їх функціонування у ЗС України, пропонується встановити (визначити) загальні та індивідуальні *показники функціонування:*

загальні – є типовими для сервісів інформаційних систем і є обов'язковими та мінімально необхідними для формування обізнаності технічного персоналу про їх поточний стан функціонування.

індивідуальні – є особливими для кожного з сервісу інформаційних систем. Вони можуть бути розроблені (застосовані) спеціально для окремо визначеного сервісу інформаційних систем, оскільки мають індивідуальні особливості.

Аномальна поведінка сервісів інформаційних систем – це їх поведінка під час функціонування, яка проявляється у випадку будь-якого впливу (зовнішнього/внутрішнього) на їх функціональні площини або безпосередньо на сам сервіс, що може трапитися у будь-який момент часу та призвести до їх функціонування за критичних умов або, як наслідок, викликати зупинку функціонування (припинення доступності для користувачів, порушення цілісності інформації або захищеності).

Для кожного сервісу інформаційної системи доцільно визначити *функціональні показники допустимого (сталого) та критичного функціонування. Показники допустимого (сталого) функціонування* – це показники, за яких сервіси інформаційних систем функціонують у межах допустимих (теоретично розрахованих або дослідно встановлених) навантаженнях та забезпечують комфортну (зручну) роботу користувачів. *Критичні показники* – це показники, за яких імовірність зупинки роботи сервісу інформаційних систем висока.

Кожен сервіс інформаційних систем повинен мати допустимий показник кількості користувачів, на яких він розрахований, або визначену кількість звернень, запитів, які вони можуть обробляти за одиницю часу. Це потрібно для того, щоб технічний персонал міг чітко орієнтуватися в питаннях оцінки якості функціонування сервісів інформаційних систем.

Сервіси інформаційних систем та їх спроможності не можуть зростати неконтрольовано. Будь-яке аномальне (відхилення від норми) функціонування (поведінка) сервісу інформаційних систем, яке обумовлене невідомими (непрогнозованими) чинниками функціонування,

необхідно розцінювати як потенціальний кібервплив (інцидент кібербезпеки), який потребує негайної фіксації (для наповнення бази знань інцидентів), його опису, спостереження ситуації, яка виникла (за необхідності), подальшого детального аналізу, класифікації, перевірки, реагування на ситуацію, що виникла, та прийняття необхідних заходів щодо захисту, усунення наслідків, відновлення функціонування. Порядок дій має бути регламентований окремими розпорядчими документами ЗС України.

З метою забезпечення сталого функціонування та оперативного реагування на зміни у роботі сервісів інформаційних систем призначається *технічний персонал*, який має бути спроможний здійснювати означені вище завдання, а саме:

управління, адміністрування – процеси забезпечення керування сервісами інформаційних систем. Полягають у виконанні керівних та розпорядчих документів, реалізації політик безпеки, інструкцій з розгортання, налаштування, відновлення, внесення змін у поточні конфігурації, проведення модернізації;

контроль технічної інфраструктури, що здійснюється шляхом аналізу інфраструктурних показників функціонування технічного майданчика відповідно до встановлених технічних вимог з необхідною обчислювальною потужністю, відповідним рівнем обслуговування та згідно з існуючими нормативно-правовими, розпорядчими документами;

контроль та управління інфраструктурою ЦОД (хмарних обчислень);

моніторинг сервісів інформаційних систем, що призначений для визначення їх поточного стану функціонування, виявлення інцидентів і проблем із конфіденційністю, доступністю, цілісністю;

протоколювання – процес формування, збору, зберігання та резервування статистичних даних технологічної інформації про результати роботи сервісів інформаційних систем. Зібрані дані в подальшому піддаються всебічному аналізу;

вимірювання функціональних показників та розрахунок середніх значень їх завантаженості, необхідний для визначення ступеня відповідності функціонування сервісів інформаційних систем до попередньо спланованих, визначених вимог та якості надання сервісу користувачам. Зібрані статистичні дані оцінюються інформаційно-аналітичними системами (персоналом, який займається інформаційно-аналітичною роботою) для визначення поточного стану функціонування сервісів інформаційних систем та прогнозування їх поведінки у майбутньому;

технічну підтримку сервісів інформаційних систем;

інформаційно-аналітичну роботу.

Окремої уваги заслуговують *чинники функціонування системи*, які можна розділити на такі:

загальні;

індивідуальні;

функціонування інженерної інфраструктури технічних майданчиків.

Розглянемо характеристики означених чинників.

Загальні чинники:

фізичні:

температурний режим роботи апаратного сегмента;

відсоток завантаженості процесорної потужності;

відсоток завантаженості оперативної пам'яті;

відсоток завантаженості та інтенсивність, швидкість використання дискового простору;

відсоток завантаженості мережевого інтерфейсу вхідного та вихідного трафіку та його доступність;

системні:

системні повідомлення про статус операційної системи як платформи для сервісу інформаційних систем;

системні повідомлення про статус сервісів інформаційних систем;

поточний час сервісу;

безпеки:

повідомлення про реєстрацію користувачів, адміністраторів сервісу;

повідомлення про зміну конфігураційних файлів, даних;

повідомлення про наявність відомих ознак компрометації;

контроль терміну дії цифрових сертифікатів;

цілісність конфігураційних складових (контенту) сервісу інформаційних систем;

контрольні:

повідомлення запланованих подій;

контроль створення резервних копій.

Індивідуальні чинники:

доступність сервісів інформаційних систем для користувачів за період часу (секунда, година, місяць, рік);

кількість користувачів сервісу;

кількість одночасних сесій користувачів;

кількість звернень до сервісу за одиницю часу та їх тривалість;

кількість і зміст успішних\неуспішних транзакцій за одиницю часу;

список і кількість процесів сервісу, тривалість їх звернень до дискового простору;

кількість звернень процесів до бази даних;

кількість процесів, що не відповідають запитам;

кількість і час помилок роботи сервісу;

геолокація запитів;

потокові процеси функціонування сервісів;

інші специфічні чинники, які можуть бути визначені додатково, індивідуально.

Чинники *функціонування інженерної інфраструктури технічних майданчиків*:

кліматичні;

чинники системи електрозабезпечення.

У свою чергу, кліматичні чинники відображають:

поточний температурний режим та відносну вологість серверного приміщення;

температурний режим роботи навколишнього середовища.

Чинники системи електрозабезпечення відображають:

контроль вхідної напруги до серверного приміщення;

поточні значення потужності, які використовується обладнанням серверного

приміщення;

поточні значення системи резервного електроживлення.

У процесі роботи системи управління і контролю функціонування сервісів доцільно використовувати поняття технологічної інформації, а також її життєвого циклу (визначення понять надаються в авторській редакції). *Технологічна інформація* – це інформація, яка формується в результаті процесу забезпечення функціонування сервісів інформаційних систем. Дані, що належать користувачам, не є технологічною інформацією. В свою чергу, *життєвий цикл технологічної інформації* – це процес її існування (життя) в інформаційних системах. Він надає чіткі відповіді на низку запитань, зокрема: як, за яких умов і яка технологічна інформація формується в результаті роботи сервісів інформаційних систем, як інформація циркулює і як вона класифікується, відбирається для аналізу, де зберігається, резервується, яким чином захищається, яким чином кому або чому надається доступ до неї, встановлюються терміни її зберігання та в обов'язковому порядку визначається порядок її виведення з системи (рис. 2).

Життєвий цикл технологічної інформації складається з чотирьох основних етапів (рис. 2):

1. Формування технологічної інформації (позначено як «Ф» на рис. 2). Етап передбачає вибір та визначення потрібної інформації про функціонування інформаційної системи. Інформація класифікується, створюються правила та критерії її відбору, визначаються алгоритми передачі, визначається порядок її захисту.

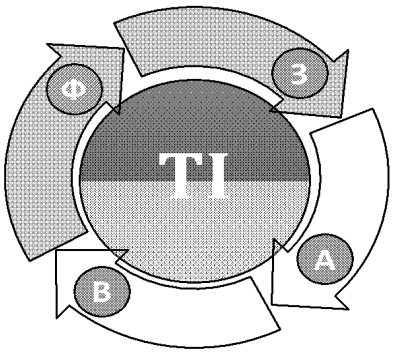

Рисунок 2 – Життєвий цикл технологічної інформації

2. Збір технологічної інформації (позначено як «З» на рис. 2). Етап передбачає формування місця зберігання технологічної інформації, строки її зберігання, резервування. Визначається порядок її захисту.

3. Аналіз технологічної інформації (позначено як «А» на рис. 2). Етап передбачає визначення порядку надання технологічної інформації технічному персоналу. Створюються механізми та правила доступу до інформації, визначається порядок її надання. Встановлюються критерії реагування на інциденти. Визначаються інформаційно-аналітичні алгоритми оцінки. Здійснюється аналіз даних.

4. Виведення технологічної інформації з функціонального циклу (позначено як «В» на рис. 2). Етап передбачає визначення порядку виведення технологічної інформації з інформаційних систем.

Крім технологічної інформації доцільно використовувати поняття *критично важлива інформація*, під яким слід розуміти всю інформацію, що належить до функціонування сервісів інформаційних систем та яка потрібна технічному персоналу для проведення операційних дій із швидкого відновлення їх функціонування, а також дані користувачів, що обробляються, зберігаються та резервуються. Ця інформація поділяється на технологічну та дані користувачів. Інформація та дані підлягають обов'язковому резервуванню.

Резервування – це процес збереження сталої версії сервісів інформаційних систем та даних користувачів. Проводиться на зовнішні або резервні сховища, резервні технічні майданчики. Призначене для унеможливлення втрати даних користувачів та технологічної інформації. Використовується у випадку відновлення сталого функціонування. Спрямоване на мінімізацію часу відновлення.

До технологічної інформації, крім інформації, що формується в результаті життєвого циклу технологічної інформації, також належать паролі, програмні сертифікати, ключі шифрування, поточні технічні конфігурації обладнання та програмних комплексів, інсталяційні пакети операційних систем, оригінали ліцензійного програмного забезпечення, вихідні коди програм, поточний дизайн вебресурсів, копії повнофункціональних сервісів на віртуальних машинах, необхідні технічному персоналу для здійснення процедури відновлення функціонування сервісу інформаційної системи у випадку припинення, відмови їх роботи в результаті виходу з ладу пасивного, активного обладнання, впливу шкідливого програмного забезпечення або відмови функціонування сервісу в результаті вдало застосованого кібервпливу.

Дані користувачів – це вся інформація, яка є результатом їх інтелектуальної діяльності, належить користувачам сервісів інформаційних систем та є власністю організації.

Процес відновлення сталого функціонування сервісу інформаційних системи є одним з найважливіших питань кіберзахисту. Технічний персонал, який забезпечує функціонування сервісів інформаційних систем повинен мати визначений, встановлений перелік критично важливої інформації та мати план резервного відновлення. Мета визначення переліку критично важливої інформації є впорядкування операційного процесу, зменшення часу відновлення сталого функціонування сервісів інформаційних систем та здійснення управління ризиками. Процес відновлення функціонування сервісів інформаційних систем має бути заздалегідь спланований та викладений у вигляді чіткої операційної процедури технічному персоналу.

Найважливішим питанням в організації роботи із резервування критичної інформації є чітке одностайне розуміння підходу до умов існування

життєвого циклу сервісів інформаційних систем. Серед загальних підходів до створення системи управління і контролю функціонування сервісів інформаційних систем у ЗС України неможливо уникнути розгляду питання підготовки персоналу.

Підготовка технічного персоналу є важливим питанням забезпечення сталого функціонування сервісів інформаційних систем. Вона має включати питання теоретичної і практичної підготовки, які безпосередньо формуються на концентрації досвіду та всебічного розвитку технічного персоналу, що забезпечує функціонування сервісів інформаційних систем.

Компетенції та необхідний рівень підготовки технічного персоналу формує власник та розробник сервісу інформаційних систем. Слід зазначити, що користувачі сервісів інформаційних систем повинні мати сформовані навички з користування сервісами, а також мати обізнаність з питань кібербезпеки та інформаційних або існуючих обмежень.

Технічна підтримка сервісів інформаційних систем (далі – ТП) є організованим функціональним процесом. Роботу ТП спрямовано на забезпечення сталого функціонування сервісів інформаційних систем та надання впорядкованої допомоги користувачам.

Технічна підтримка передбачає наявність:

навченого персоналу;

спеціально підготовлених автоматизованих робочих місць та систем відображення інформації;

програмних інструментів сервісів управління і контролю;

адміністративних та організаційно-розпорядчих документів, інструкцій (операційних процедур);

пунктів технічної допомоги користувачам (ServiceDesk).

Під час організації роботи ТП потрібно чітко розуміти:

функціональні ролі учасників процесу ТП та їх зони відповідальності;

ієрархію побудови ТП та процеси взаємодії ліній технічної підтримки;

чіткі операційні процедури (інструкції) з порядку надання або відновлення доступу користувачів до сервісів інформаційних систем;

необхідність впорядкування звернень шляхом створення єдиної інформаційної точки входу усіх запитів (звернень) користувачів;

наявність якісно підготовленого технічного персоналу ТП;

необхідність застосування програмних платформ для організації та функціонування ТП.

Технічна підтримка поділяється на дві основні категорії:

ТП пунктів управління, що охоплює в собі технічний персонал, задіяний для забезпечення доступу до сервісів інформаційних систем на пунктах управління, в місцях постійної дислокації або окремих користувачів та їх забезпечення програмними і технічними засобами. Додатково можуть розгортатися окремі пункти технічного забезпечення користувачів (Service Desk).

ТП рівня формування сервісів, що охоплює в собі технічний персонал, задіяний у формуванні сервісів інформаційних систем, їх адмініструванні та підтримці технічного супроводження функціонування.

ТП має чотири лінії підтримки. Кожна лінія має чітко визначені повноваження та призначення.

Перша лінія ТП призначена для:

приймання, фіксації інцидентів, звернень, які надходять від користувачів сервісів інформаційних систем;

надання консультативної допомоги користувачам з порядку доступу до сервісів інформаційних систем;

надання технічної допомоги із доступу до сервісів інформаційних систем та координації дій особового складу технічного персоналу пунктів технічного забезпечення користувачів;

ескалації розгляду питання інцидентів та звернень користувачів до ІІ лінії ТП, які мають вищі повноваження із адміністрування сервісів інформаційних систем з метою залучення більш кваліфікованих технічних спеціалістів.

Ця лінія ТП створюється з метою безпосередньої роботи з користувачами, оскільки на практиці саме користувачі є джерелом постійного формування уваги та питань, які найчастіше повторюються. Формування першої лінії ТП дає змогу більш кваліфікованим спеціалістам надавати належну увагу для безперебійного функціонування сервісів інформаційних систем.

Друга лінія ТП працює на рівні користувач–пункт управління, може бути задіяна для вирішення завдань рівня у випадку, коли перша лінія ТП не змогла самостійно вирішити питання, а звернення користувача або інцидент потребують залучення технічного персоналу з вищим рівнем кваліфікації.

Третя лінія ТП працює виключно на рівні пункту управління, призначена для вирішення технічних питань вищого рівня складності у випадку, якщо друга лінія ТП не в змозі їх вирішити самостійно, а звернення користувача або інцидент, проблема потребують залучення технічного персоналу з вищим рівнем кваліфікації. Це найдосвідченіший технічний персонал організації.

Четверта лінія ТП призначена для вирішення технічних питань найвищого рівня складності у випадку, якщо третя лінія ТП не в змозі їх вирішити. Зазвичай це розробники сервісів інформаційних систем, вендори обладнання, які вирішують проблеми, пов’язані із застосуванням технологій, які залучені до функціонування сервісів інформаційних систем.

З метою забезпечення сталого функціонування сервісів інформаційних систем повинна проводитись *інформаційно-аналітична робота* (далі – ІАР), що є невід’ємною частиною супроводження роботи системи. ІАР призначена для аналізу поточного стану функціонування сервісів інформаційних систем, прогнозування їх поведінки у майбутньому та визначення ступеня відповідності сервісів інформаційних систем меті і завданням, що на них покладені.

На ІАР покладаються такі завдання:

здійснення аналізу функціонування сервісів інформаційних систем на постійній основі;

формування звітів з функціонування сервісів інформаційних систем;

фіксація, опис та документування аномальних поведінок, інцидентів та проблем, які виникають під час функціонування сервісів інформаційних систем;

ведення бази знань інцидентів та проблем;

визначення поточного ступеня відповідності функціонування сервісів інформаційних систем встановленим (визначеним) для них меті і завданням;

координація роботи технічної підтримки сервісів інформаційних систем, яка спрямована на всебічне покращення обслуговування абонентів;

оцінка показників чинників функціонування;

прогнозування поведінки сервісів інформаційних систем на короткострокову перспективу (у поточному та наступному роках). Прогнозування здійснюється з метою недопущення припинення функціонування сервісів інформаційних систем у майбутньому;

формування пропозицій щодо покращення функціонування сервісів інформаційних систем;

оцінка ризиків функціонування сервісів інформаційних систем та управління ними.

Інцидент – це факт виявленої аномальної поведінки сервісів інформаційних систем під час їх функціонування, вирішення якого відбувається на рівні технічного персоналу та не потребує тривалого часу або додаткових ресурсів. Інцидент може стати причиною відмови або припинення надання сервісів інформаційних систем користувачам.

Проблема – це ситуація, яка, як правило, виникає у результаті частого виникнення інцидентів, вирішення якої потребує тривалого часу, залучення кваліфікованих спеціалістів або додаткових ресурсів. Проблема може стати причиною відмови або припинення надання сервісів інформаційних систем користувачам.

База знань інцидентів та проблем – це класифікований інформаційний каталог, який містить хронологічний список та опис всіх інцидентів та проблем, що виникли за весь час функціонування сервісів інформаційних систем. Призначена для протоколювання інцидентів та проблем, виявлення схожих за типом ситуацій та є інструментом інформування технічного персоналу, який використовує її для зменшення часу на відновлення функціонування сервісів.

Тому сервіси можуть бути модифіковані на конкретному етапі життєвого циклу сервісу інформаційної системи. Це відбувається, коли військова структура (військова адміністрація, організація, установа, орган управління) змінює свою місію або змінює свої можливості для досягнення певних операційних цілей. Під час використання послуг інформаційної системи необхідно оцінювати спроможності кожного конкретного користувача, що, в свою чергу, дає розуміння можливості вирішення проблеми кількома способами і вибором серед них найоптимальнішого.

Механізми оцінювання, в обов'язковому порядку, приймаються установою (організацією), в інтересах якої функціонують сервіси інформаційних систем. Оцінювання здійснюється з метою визначення ефективності спроможностей та відповідності їх цінності, яка визначена організацією в межах споживання відповідних сервісів. Якщо цінності установи (організації) змінюються, відповідно повинні змінюватися сервіси інформаційних систем разом зі спроможностями користувачів, які вони набувають під час використання (споживання) сервісів.

Висновки і перспективи подальших досліджень

Таким чином, сервіси інформаційних систем широко використовуються службовими особами Збройних Сил України у своїй повсякденній діяльності. Мета їх застосування полягає в автоматизації (цифровізації) функціональних процесів – (робочих процесів оперативних спроможностей) у Збройних Силах України та досягненні ефективних (бажаних) результатів, цілей за найменш короткий проміжок часу з максимально можливою ефективністю. Сервіси інформаційних систем мають забезпечувати максимально зручне та надійне (стале) функціонування в інтересах Збройних Сил України. Вони мають вирішувати лише ті завдання, які на них покладені, відповідати їх функціональному призначенню. Кожен сервіс інформаційних систем являє собою цінність для кінцевого користувача та для організації в цілому, а споживання (використання) сервісів формує спроможності.

Запропоновані у статті функції та інформаційні зв'язки у процесі використання сервісів інформаційних систем, які відображені на функціональній моделі (рис. 1), дають змогу визначити та стандартизувати загальні підходи щодо створення та функціонування системи управління і контролю функціонування сервісів інформаційних систем, які застосовуються з метою автоматизації (цифровізації) процесів управління в Збройних Силах України, і таким чином – створити підґрунтя для впровадження архітектурного планування інформаційних технологій у Збройних Силах України.

Напрямами подальших досліджень є формування методичного апарату оцінювання ефективності функціонування системи управління і контролю функціонування сервісів інформаційних систем різного призначення.

Список бібліографічних посилань

1. ДСТУ 2392-94. Інформація та документація. Базові поняття. [Чинний від 01.01.1995]. Вид. офіц. Київ : Держспоживстандарт України, 1994. 26 с. **2. Про захист інформації в інформаційно-комунікаційних системах** : Закон України від 05.07.1994 № 80/94-ВР. URL: pttps://zakon.rada.gov.ua/laws/spow/80/94-%D0%B2%D1 % 80#Text (дата звернення: 12.10.2023). **3. Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах** : Постанова КМУ від 16.11.2002 № 1772 URL: https://zakon.rada.gov.ua/laws/show/1772-2002-%D0%BF#Text (дата звернення: 12.10.2023). **4. ДСТУ ISO/IEC/IEEE 42010:2018.** Інженерія систем і програмних засобів. Опис архітектури (ISO/IEC/IEEE 420010:2010). [Чинний від 15.08.2018]. Вид. офіц. Київ :

ДП «УкрНДНЦ», 2018. **5. Allied Joint Doctrine for Communication sand Information Systems (Edition A Version 1)** Союзна об'єднана публікація НАТО AJP-06. [Чинний від 06.04.2011]. **6. ВСТ 01.109.004-2003 (01)**. Інформатизація Збройних Сил України. Інформаційно-аналітична система Збройних Сил України. Терміни та визначення [Чинний від 28.02.2003]. 2003. 32 с. **7. ВКП 6-00(01).01**. Військова керівна публікація військовим організаційним структурам зі зв'язку та інформаційних систем. Доктрина «Зв'язок та інформаційні системи», затверджена Головнокомандувачем ЗС України 01.07.2020. 75 с.

GENERAL APPROACHES OF CREATING A SYSTEM OF MANAGEMENT AND CONTROL OF FUNCTIONING OF INFORMATION SYSTEMS SERVICES IN THE ARMED FORCES OF UKRAINE

Panchenko Serhiy [1]
Antoniuk Andrii [2]
Novytskyi Dmytro [1]
Usok Serhii [2]
Zamorskiy Serhii [2]

[1] ***Kruty Heroes Military Institute of Telecommunications and Information Technologies, Kyiv, Ukraine***
[2] ***J6 General Staff of the Armed Forces of Ukraine, Kyiv, Ukraine***

Formulation of the problem in general. *The purpose of this paper is to develop unified approaches to the use of information systems management and control services in a service-oriented environment of the communication and information systems of the Armed Forces of Ukraine, as well as to create the basis for the implementation of IT architectural planning in the Armed Forces of Ukraine. The relevance of the topic of the material presented is justified by the level of modern development of the management system of the Armed Forces of Ukraine and its material and technical base - the communication system, which, in turn, has long gone beyond the requirements for ensuring pure communication.*

Analysis of recent researches and publications. *The governing documents for the creation and implementation of information systems are the Laws of Ukraine, resolutions of the Cabinet of Ministers of Ukraine, orders and instructions of the Ministry of Defense of Ukraine, the Commander-in-Chief of the Armed Forces of Ukraine, the Chief of the General Staff of the Armed Forces of Ukraine, and other doctrinal and managerial documents in various fields of activity.*

Presenting the main material. *Various information systems continue to be implemented and expanded in the Armed Forces of Ukraine in order to ensure parity in the face of an insidious enemy, increase the effectiveness of the use of weapons and military equipment, and obtain an information advantage during decision-making in the process of managing troops. Services of information systems are widely used by officials of the Armed Forces of Ukraine in their activities. The purpose of their application is to automate (digitalize) functional processes in the Armed Forces of Ukraine and achieve effective (desired) results and goals in the shortest possible time with maximum possible efficiency. The purpose of their article is to automate (digitalize) functional processes in the Armed Forces of Ukraine and achieve effective (desired) results and goals in the shortest possible time with maximum possible efficiency.*

Elements of scientific novelty. *The article proposes the general approaches of creating a system of management and control of the functioning of information systems services in the Armed Forces of Ukraine, which are based on the experience of using military units (units), and also correspond to the best global practices in the use of information technologies. The necessary conceptual apparatus for the existence of information system services is presented. The article presents a functional model of the system of management and control of the functioning of services, which introduces a system of information connections between functional modules and determines the content of technological information that will circulate in it.*

Practical significance of the article. *The proposed model makes it possible to form and standardize an approach to building a management system and monitoring the functioning of information system services, which are used for the purpose of automation (digitalization) of management processes in the Armed Forces of Ukraine.*

Conclusion and the perspectives of future researches. *The perspective of future researches is the development of a methodological apparatus for assessing the efficiency of the functioning of the system for managing and controlling the functioning of information systems services for various purposes.*

Keywords: *information technologies, communication system, information systems, information services, services for management and control of information systems.*

References

1. DSTU 2392-94. Information and documentation. Basic concepts. [Chynnyj vid 01.01.1995]. Vyd. ofits. Kyiv : Derzhspozhyvstandart Ukrainy, 1994. 26 s. **2. About** the protection of information in information and communication systems : Zakon Ukrainy vid 05.07.1994 № 80/94-VR. URL: https://zakon.rada.gov.ua/laws/show/ 80/94-%D0%B2%D1% 80#Text (data zvernennia: 12.10.2023) **3. Procedure** for interaction of executive authorities on issues of protection of state information resources in information and telecommunication systems : postanova Kabinetu Ministriv Ukrainy vid 16.11.2002 № 1772. **4. DSTU ISO/IEC/IEEE 42010:2018**. Systems and software engineering — Architecture description (ISO/IEC/IEEE 420010:2010). [Chynnyj vid 15.08.2018]. Vyd. ofits. Kyiv : DP «UkrNDNTs», 2018. **5. Allied** Joint Doctrine for Communication sand Information Systems (Edition A Version 1) Soiuzna ob'iednana publikatsiia NATO AJP-06. [Chynnyj vid 06.04.2011]. **6. VST 01.109.004-2003 (01)**. Informatization of the Armed Forces of Ukraine. Information and analytical system of the Armed Forces of Ukraine. Terms and definitions. [Chynnyj vid 28.02.2003]. 2003. 32. **7. VKP 6-00(01).01**. Military guidance publication for military organizational structures on communications and information systems. Doctrine «Communication and information systems», zatverdzhena Holovnokomanduvachem ZS Ukrainy 01.07.2020, 56.