Khoroshko Volodymyr, doctor of technical sciences, professor, professor of the department of security of information technologies of the National Aviation University.
E-mail: professor_va@ukr.net.
Orcid ID: 0000-0001-6213-7086.

Хохлачова Юлія Євгеніївна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
Khokhlacheva Yuliya, candidate of technical sciences, associate professor, associate professor of the department of security of information technologies of the National Aviation University.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

Погорелов Володимир Володимирович, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
Pogorelov Volodymyr, Candidate of Technical Sciences, Associate Professor of the Department of Security of Information Technologies of the National Aviation University.
E-mail: volodymyr.pogorelov@gmail.com
Orcid ID: 0000-0002-6100-1504.

DOI: 10.18372/2410-7840.24.16861
УДК 621.382

ЗАСТОСУВАННЯ МЕТОДІВ ТЕХНІЧНОГО ДІАГНОСТУВАННЯ ПРИ РОЗВ'ЯЗАННІ ЗАВДАНЬ КІБЕРНЕТИЧНОГО ЗАХИСТУ

Василь Кузавков

В статті обґрунтовується можливість застосування діагностичної інформації на основі фізико-хімічних процесів в напівпровідникових структурах програмно-апаратних засобів - систем з вбудованим програмним забезпеченням сучасних телекомунікаційних систем для розв'язання задач кібернетичного захисту. Предметом дослідження виступає процес функціонування сукупності технічних засобів прийому, передачі, збереження та обробки даних під управлінням (керівництвом) програмної складової (сукупність технічних засобів, які є практичною реалізацією моделі OSI). Наведено узагальнена схема взаємодії програмної та апаратної складової обраного типу радіоелектронного устаткування та особливості застосування фізичного підходу до контролю технічного стану цього устаткування для розв'язання задач кіберзагроз, кібератак. До завдань технічного діагностування відносимо контроль за змінами стану апаратної частини (внаслідок старіння або підміни) так і змінами в програмному забезпеченні (внаслідок збоїв або втручання сторонніх осіб). В будь якому разі, задачі які вирішуються, пов'язані з оцінкою фактичного стану програмно – апаратних засобів, прогнозом на майбутнє, оцінкою ймовірностей настання відмов, ризику аварійних ситуацій. На основі аналізу значень діагностичного параметру (порівнянні його з еталонними або розрахунковими) встановлюється місце невідповідності встановленому (визначеному) режиму функціонування, причини та можливі наслідки. Прийняття рішення принципово можливий в разі наявності діагностичного параметру, наявності адекватної моделі об'єкту контролю (для отримання розрахункових даних), або достатньої для статистичної обробки кількості однотипних засобів з однаковими умовами функціонування. Фізичні підходи методів технічного діагностування запропоновано використовувати для вирішення наступних завдань: ідентифікація та автентифікації телекомунікаційного устаткування; визначення нетипового навантаження на програмному рівні. Завдання підвищення інформаційної безпеки також обумовлює необхідність пошуку (розробки) або створення пристроїв, які здатні генерувати електричні сигнали випадкового (шумового) характеру. В якості основного методу розглядається безконтактний індукційний метод.

Ключові слова: *діагностичний параметр, фізико-хімічні процеси, радіоелектронне обладнання, модель, прогнозування.*

ВСТУП

Під кібератакою розуміємо навмисні дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій та спрямовані на досягнення цілей: порушення конфіденційності, цілісності, доступності електронних інформацій-

них ресурсів комунікаційних систем, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування систем; використання комунікаційної системи, та засобів електронних комунікацій для здійснення кібератак на інші об'єкти.

Кібернетичний захист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем. [1] В свою чергу, технічна діагностика - теорія, методи і засоби виявлення дефектів об'єктів технічної природи. Завданнями технічного діагностування є перевірка справності, працездатності і правильності функціонування машини, а також пошук і прогнозування розвитку дефектів, що перешкоджають або знижують ефективність виконання машиною її функцій.

Кібернетичний захист (так само як і діагностика) необхідний на всіх етапах життєвого циклу технічної системи: при проектуванні і доведенні дослідного зразка, при виробництві серійної продукції, у періоди експлуатації і ремонту. Алгоритми, методики і методи, які застосовуються на кожному з етапів, можуть відрізнятися один від одного. Це пояснюється відмінностями виду деструктивного впливу на систему, їх природою і необхідною глибиною контролю.

Найбільший ефект від використання запропонованих методів досягається на етапі експлуатації за рахунок прогнозування та усунення можливих наслідків деструктивного впливу, пов'язаних з цим простоїв, виключення раптових аварійних зупинок обладнання, скорочення термінів, вартості і обсягу відновлення системи. Крім того, необґрунтоване втручання в роботу системи прискорює знос устаткування, здатне вносити нові непередбачені впливи, які скорочують термін служби устаткування і вимагають нових робіт по відновленню та налаштуванню.

В основу різних методів і способів діагностування покладене вимірювання фізичних параметрів. При цьому, в залежності від об'єкту контролю, використовують: електрометрію, віброакустику, дефектоскопію, інтроскопію, вимірювання механічних властивостей, складу речовини, розміру, сил, деформацій, тиску, температури, часу, маси, вологості, рівня. Для цього використовують широку номенклатуру випробувальної техніки, приладів і устаткування відповідного класу точності [2].

Дослідження сигналів отриманих не з контрольних точок внаслідок виконання радіоелектронною системою своїх функцій (або спеціально підготовленого тесту) показало, що ці сигнали корелюють зі вхідним впливом, сугубо індивідуальні для кожного зразку техніки, цілком інформативні і придатні для використання як при вирішенні завдань технічного діагностування так і задач кібернетичного захисту. Джерелом подібної інформації у радіоелектронних (телекомунікаційних) системах можуть бути різні фізичні явища (наприклад, шум у радіоелектронних приладах), системні джерела (стан і події програмного середовища – системний час, мережева активність, переривання), джерела засновані на інтерактивній діяльності оператора (руху мишею, натискання клавіш). Одне з джерел – шумоподібні сигнали отримані безпосередньо в ланцюгах живлення з подальшим визначенням їхніх імовірнісних (статистичних) показників [3].

Як відмічалося, завдання підвищення інформаційної безпеки обумовлює необхідність пошуку (розробки) або створення спеціалізованих пристроїв, які здатні генерувати електричні сигнали випадкового (шумового) характеру, а сигнали від фізичних джерел мають кращі випадкові характеристики [4]. Технічна діагностика також знаходиться в пошуку нових джерел інформаційних (діагностичних) сигналів. Можливість застосування методів технічного діагностування обумовлена спорідненістю процесів які спричиняють зміни технічного стану (зміни відображуються в значеннях обраного діагностичного параметру) під деструктивним впливом (кібератакою).

Сутність запропонованого підходу полягає в використанні спеціально підготованих перевірних послідовностей для отримання інформаційного (з точки зору діагностування) фізичного відгуку системи (об'єкту контролю) та безконтактного вимірювання цього відгуку в єдиній для всієї системи точці [5].

Відомо, що процес кібернетичного захисту (в технічному аспекті) так само як і визначення технічного стану об'єкту контролю заснований на вимірюванні, аналізі та екстраполяції явищ на майбутній час за відомими результатами спостережень (за відповідними явищами в попередній період). Параметрами, які використовуються для

оцінки поточного технічного стану об'єкту контролю, можуть бути:

- експлуатаційні параметри, які вимірюються вбудованими пристроями контролю (функціональна діагностика) без переривання циклу функціонування устаткування;
- параметри технічного стану, які вимірюються зовнішніми приладами (автономними системами контролю технічного стану) із припиненням циклу функціонування.
- параметри технічного стану, які вимірюються зовнішніми приладами (автономними системами контролю технічного стану) без припинення циклу функціонування – тестовий контроль.

Існує підхід до прийняття рішення про поточний стан технічного ОК заснований на імовірнісних методах оцінки результатів контролю, та на фізичних передумовах функціонування об'єкту контролю [6-8]. Застосування імовірнісних методів вимагає виконання умови статистичної стійкості [8]. Оцінка ресурсу унікального обладнання, існуючого в одиничному виконанні або в умовах обмеженої кількості дещо ускладняється. Умови статистичної стійкості, використання імовірнісних методів сумнівні.

Застосування фізичних передумов до функціонування РЕО та визначення технічного стану до недавнього часу не дозволяло врахувати різноманіття реальних умов експлуатації [6]. Розвиток методології технічного діагностування змінив це становище. Застосування теорії дефектоутворення в напівпровідникових структурах, виникнення нових безконтактних методів збору інформації, реєстрації стохастичних процесів зміни струму в напівпровідникових структурах під час функціонування об'єкту контролю, можливість створення функціональних тестів активації окремих апаратних частин устаткування (навіть дистанційна) дозволяють не лише вирішувати основні задачі технічної діагностики, а і задачі кібернетичної безпеки. [9,10]. Додатковими умовами є створення (та перевірка в ході прискорених випробувань) математичних моделей радіоелектронних компонентів (РЕК), вибір ефективного діагностичного параметру [11,12]. Все це дозволяє не лише розв'язувати задачі технічного діагностування, а і задачі кібернетичного захисту сучасних телекомунікаційних систем.

ОСНОВНА ЧАСТИНА

Серед задач, які вирішуються технічною діагностикою є: визначення технічного стану; локалізація несправностей; прогнозування технічного стану об'єкту контролю. Отримані дані застосовуються з метою попередження аварійних станів та для скорочення часу відновлення працездатного стану об'єкту контролю.

Враховуючи особливості обраного для досліджень об'єкту контролю (кількісну розмірність, територіальне рознесення, різноманіття технічних засобів), прийняття рішення в реальному часі без застосування автоматизованих систем контролю (діагностування) неможливо [13]. Окрім того, в складі системі діагностування необхідне застосування елементів системи підтримки прийняття рішень [14].

Структурна схема, яку наведено на рис. 1, пояснює процес розв'язання задач технічного діагностування в системі однотипних програмно-апаратних засобів (ОК). Представлено умовний тракт проходження інформаційних (перевірних) повідомлень та основні складові діагностичного параметру в системах, побудованих за моделлю OSI.

Діагностичний параметр в цьому випадку містить в собі дві складові: енергетичну та часову. Енергетична складова обумовлена функціонуванням апаратної частини устаткування (кількісний та якісний склад апаратної частини яка присутня в тракті обміну інформації), визначається змістом заголовка тестового повідомлення. Часова складова обумовлена функціонуванням програмної частини (часом необхідним на опрацювання заголовків та формування відповіді на тестове повідомлення).

При цьому, вирішення задач як технічного діагностування так і кібернетичної безпеки спрямовано на визначення джерел деструктивного впливу або деградації якості (в апаратній і в програмної частини), виявлення підміни елементів апаратної частини, розгалужень в трактах передачі інформації, впливу зловмисного програмного забезпечення. В обох випадках обраний ДП має інформативний характер.

На рис. 1. позначено: $y(t,\tau)$, $y_{ет}(t,\tau)$ – виміряне значення діагностичного параметру та еталонне значення двоскладового діагностичного параметру (ДП). Отримані значення індивідуальні та неповторні.

Неповторність пов'язана з особливостями фізико-хімічних процесів старіння напівпровідникових структур в зразках РЕО. Чисельне значення діагностичного параметру залежать від

конструктивних параметрів апаратної складової об'єкту контролю h', амплітудної та фазочастотної характеристики тракту формування та передачі повідомлень.

Час напрацювання об'єкту контролю – t; τ – тривалості перевірних тестових послідовностей; $\Delta\tau_\Sigma = \Delta\tau_1 + \Delta\tau_1' + \Delta\tau_2$ – сумарне приростення часу; $\Delta\tau_1$, $\Delta\tau_1'$ – часове приростення, пов'язане з функціонуванням апаратної частини об'єкту контролю; $\Delta\tau_2$ – приростення часу, яке характеризує затримки, обумовлені дисципліною обслуговування (обробки) тестових повідомлень, вплив параметрів налаштування програмного середовища - h.

Слід відзначити, що складова $\Delta\tau_2$ також відображує в собі характерні особливості апаратної частини h' (обсяг пам'яті, частота процесору, частота опитування пристроїв вводу-виводу і т. ін.), оскільки обчислювальні процеси виконуються відповідною апаратною частиною.

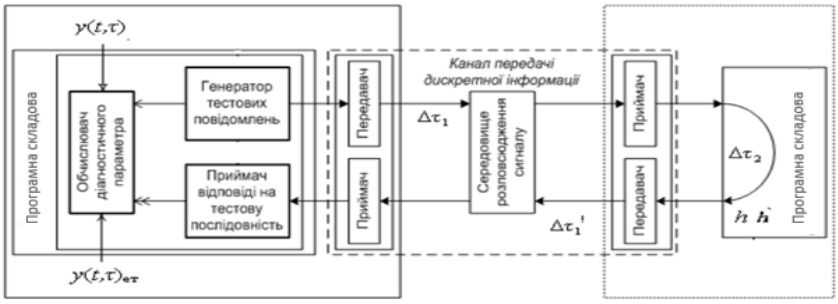

Рис. 1 Схема проходження перевірних тестових послідовностей у системах з підтримкою моделі OSI

Нехай основні функціональні властивості об'єкту контролю характеризуються оператором L, який пов'язує вхідні і вихідні сигнали $U(t)_{вх}$ і $U(t)_{вих}$, конструктивні параметрі h, h' а також враховує залежність вихідного сигналу $U(t)_{вих}$ від фактору збудження $\Delta U(t,\tau)$, який, в свою чергу, породжений спеціально підготовленим вхідним перевірним тестом та має ознаки тривалих (t) та швидких (τ) процесів. Під вихідним сигналом розуміємо діагностичний сигнал, або сигнал з датчика діагностичної інформації. В запропонованому методі це сигнал з безконтактного індукційного датчика.

Показником функціонування об'єкту контролю є діагностичний параметр $y(t,\tau)$ (зміна технічного стану об'єкту визначається за стохастичними змінами струму в шині живлення об'єкту контролю) [6] залежить не тільки від конструктивних параметрів h та перевірних тестових послідовностей тривалістю τ, а і від часу напрацювання об'єкту контролю t та пов'язаними з ним фізико-хімічними процесами в напівпровідникових структурах об'єкту контролю.

Узагальнена схема діагностичної моделі представлена на рис 2.

Визначений об'єкт контролю (діагностування) складається з взаємопов'язаних частин: апаратної (конструктивні параметрі h') та програмної, яка визначає алгоритм функціонування апаратної частини (конструктивні параметрі h). Тому в запропонованому діагностичному параметрі присутні дві складові: перша – енергетична (визначається за стохастичними процесами зміни струму, друга – часова для відображення змін часу виконання елементарних функцій при опрацюванні вхідної тестової послідовності.

Оператор Q пов'язує між собою параметри h (склад апаратної частини) та вхідні перевірні тести (з тривалістю τ). Параметр $r(\tau)$ відображає вплив програмної складової на апаратну складову об'єкту контролю. Оператор W пов'язує між собою конструктивні параметри h' (склад програмних модулів або елементарних функцій), вплив керуючої програмної складової $r(\tau)$, та енергетичну складову діагностичного параметру $y(t,\tau)$. Оператор T введено для поєднання та відображення внеску обох конструктивних параметрів об'єкту контролю h, h' (програмного та апаратного) у фактор збудження $\Delta U(t,\tau)$ (поєднання операторів операторами Q та W).

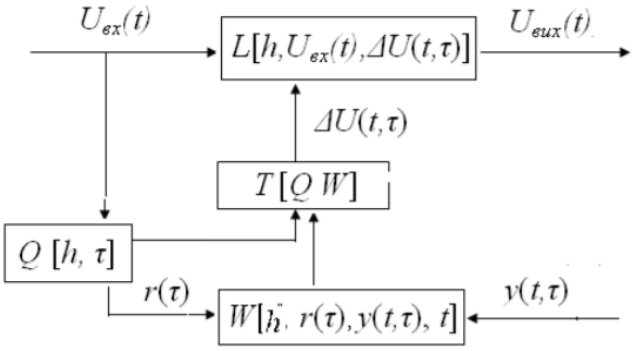

Рис. 2. Узагальнена схема моделі взаємодії програмної та апаратної частини об'єкту контролю

Зміна параметрів енергетичної складової діагностичного сигналу в результаті старіння (за часом) відбувається значно повільніше, в порівнянні з флуктуаціями основних експлуатаційних (функціональних) показників. Динаміка зміни діагностичного параметру досліджується протягом усього життєвого циклу об'єкту контролю. Отже, представлена модель враховує два види процесів, які відбуваються в тракті проходження тестових повідомлень телекомунікаційної системи: швидкі τ – флуктуація експлуатаційних (функціональних) показників і повільні t – розвиток дефектів в напівпровідникових структурах. Швидкі процеси визначають технічний стан об'єкта контролю на момент діагностування (в момент часу контролю), а повільні – параметричну надійність об'єкту контролю.

Таким чином, за результатами контролю технічного стану телекомунікаційної системи (за результатами застосування безконтактного індукційного методу, спеціальної перевірної послідовності, порівняння отриманого результату з еталоном) можливо оцінити фактичний технічний стан ОК, локалізувати місце деградації якості системи, спрогнозувати технічний стан на певний проміжок часу.

Прогнозування технічного стану з точки зору кібернетичної безпеки означатиме передбачення чисельного значення діагностичного параметру під час чергової перевірки об'єкту контролю з врахуванням індивідуального процесу старіння напівпровідникових структур в складі ОК, що ускладнює фізичне втручання або підміну устаткування.

Залежно від математичного апарату, який застосовується, в теорії прогнозування розрізняють: експертні оцінки; аналітичні оцінки (розрахунки); імовірнісні (визначається ймовірність виходу (невиходу) параметру або параметрів ТС за допустимі межі); статистична класифікація, або розпізнавання образів (внаслідок прогнозування визначається клас об'єкту діагностування за критерієм працездатності) [6, 8].

В свою чергу, параметри технічного стану бувають прямі (безпосередньо характеризують конкретні властивості об'єкту або його складової частини) і непрямі (пов'язані з прямими детермінованою або стохастичною залежністю). Застосування не прямих параметрів можливо з урахуванням низки умов:

- відомі фізичні процеси, які призводять до ресурсних відмов, а також математичні моделі зміни прямих (структурних) і непрямих (діагностичних) параметрів;
- для кожного прямого ПТС встановлені граничні значення, досягнення яких визначає величину ресурсу за цим параметром;
- в процесі спостереження за зміною технічного стану виробу є можливість фіксації параметрів, які відображають індивідуальні особливості об'єкту контролю;
- існує інформація про функціональні або регресійні співвідношення між прямими і непрямими ПТС; – залежність між математичними очікуваннями прямих і непрямих ПТС є монотонною і неперервною.

У випадку прогнозування технічного стану визначення ресурсу (за непрямими ПТС) супроводжується трьома видами похибок: похибками вимірювання непрямих параметрів; похибками, пов'язаними з випадковою природою фізичних процесів розвитку відмов; методичними похибками визначення прямих ПТС за значеннями непрямих.

При цьому, залежно від обсягу наявної інформації щодо об'єкту контролю, можливі три групи типових ситуацій.

Перша група: – відомий вид функції F , яка визначає зв'язок між прямим і непрямим параметрами, та усі коефіцієнти і дисперсії цих коефіцієнтів; – існують результати періодичних вимірювань непрямого параметру.

Друга група: – вид функції F відомий, коефіцієнти невідомі; – існують результати періодичних вимірювань непрямого параметру та результати навчального експерименту, в процесі якого відбувається одночасне вимірювання прямого і непрямого ПТС.

Третя група: – функція F монотонна і неперервна (загальний вид невідомий); – існують результати навчального експерименту. Дисперсія оцінки ресурсу представлена у вигляді суми трьох доданків: похибки вимірювань; похибки визначення коефіцієнтів функції F ; похибки визначення дисперсії випадкової зміни збільшення параметру контролю.

Застосування відомих співвідношень ускладняється необхідністю значного обсягу попередніх досліджень для встановлення вихідних даних.

Найбільш доступним для практичного використання є метод, заснований на степеневій апроксимації зміни ПТС. Прогнозування технічного стану принципово можливе лише в разі наявності інформаційного діагностичного параметру та адекватної діагностичної моделі об'єкту контролю. Для наочності на рис. 3 представлено графік зміни енергетичної складової діагностичного параметру (зміни концентрації основних носіїв в напівпровідникових структурах) під час експлуатації (життєвого циклу РЕО).

Використовуються наступні позначення: $I_{дп}$ – енергетична складова діагностичного параметру (струм), $t_{кр}$ – критичній час напрацювання; 1 – експериментальна крива, 2 – аналітична крива, 3 – приклад наявності в системі елементів з деградацією якості, або підміни устаткування. В роботах [11, 12] наведено результати порівняння (умови порівняння) натурних випробувань з результатами розроблених аналітичних діагностичних моделей радіоелектронного компоненту (РЕК), з яких складаються зразки РЕО. Аналітична модель (РЕК) (модель зміни діагностичного параметру) отримана з урахуванням фізико-хімічних процесів, які відбуваються в напівпровіднику протягом часу його експлуатації. Результатом натурних випробувань (форсованих випробувань), в основі яких лежить сукупність теоретично та експериментально обґрунтованих закономірностей та допущень, є математичне очікування динаміки зміни діагностичного параметру. Внаслідок порівняння результатів, отриманих аналітично та експериментально, визначено ступінь їх подібності з урахуванням відносної похибки моделювання.

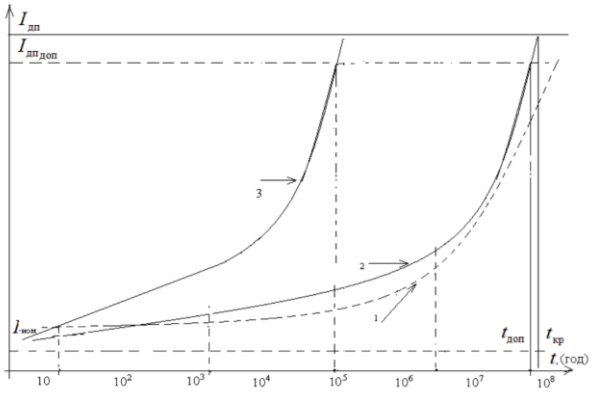

Рис. 3. Зміна енергетичної складової діагностичного параметру (фізичного прояву діагностичного параметру) під час життєвого циклу ОК.

В свою чергу, часова складова в запропонованому для програмно-апаратних засобів діагностичному параметрі, також має певну динаміку змін, обумовлених надійнісними показниками програмного забезпечення, які можуть бути виміряні у відгуку системи на спеціальний перевірний тест.

ВИСНОВКИ

На сьогодні існує багато зразків та систем РЕО, для яких характерна наявність програмної та апаратної складової (сукупність технічних засобів прийому, передачі, збереження та обробки даних під управлінням програмної складової). Особливості таких систем (складність, чисельність, розмірність в тому числі геометрична розмірність і т.ін.) вимагає застосування автоматизованої системи діагностування.

Схожість завдань та умов технічного діагностування та кібернетичної безпеки дозволяє стверджувати про можливість використання методів технічного діагностування для розв'язання задач кібернетичної безпеки.

На нашу думку, найбільш перспективним є безконтактний індукційний метод заснований на використанні узагальненого діагностичного параметру та спеціально підготовлених перевірних тестових послідовностей.

Використання запропонованого підходу до контролю технічного стану сукупності технічних засобів прийому, передачі, збереження та обробки даних під управлінням програмної складової (сукупність технічних засобів, які є практичною реалізацією моделі OSI) дозволить не скоротити число відмов РЕО в процесі експлуатації, виключити позапланову (аварійну) зупинку, заощадити кошти на відновлення, збільшити міжремонтний період напрацювання, а також вирішити завдання контролю фізичної цілісності цих систем – завдань кібернетичного захисту.

Напрямком подальших досліджень є:

– встановлення динаміки зміни узагальненого енергетично часового діагностичного параметру;

– визначення та обґрунтування припустимих меж цього параметру в двомірної площині;

– використання отриманої інформації для обґрунтування періодичності контролю однотипних програмно-апаратних засобів як одного з видів сучасних об'єктів РЕО.

ЛІТЕРАТУРА

[1] Закон України Про основні засади забезпечення кібербезпеки України https://zakon.rada.gov.ua/laws/show/2163-19#Text.

[2] Генкин М. Д., Соколова А. Г. Виброакустическая диагностика машин и механизмов. –М.: Машиностроение, 1987. – 282 с.

[3] Кузавков В. В. Оцінка ймовірносних характеристик джерел випадкових сигналів. // сучасна спеціальна техніка. – 2021. – №2. – С. 19-28.

[4] Ершов, Д.Ю. Техническое диагностирование и методы контроля механических узлов в машиностроении. – Москва, 2013. – № 4. – С. 62-64.

[5] Кузавков В. В., ГІ Гайдур, С.О. Серих, Є.В. Редзюк Безконтактний індукційний метод визначення технічного стану цифрового блока: розрахунок потужності випромінювання провідника // Зв'язок. – 2016. – №1. – С. 32-39.

[6] Стрельников, В.П. Состояние и перспективы теории и практики надежности. Надежность и долговечность машин и сооружений: Международный научно-технический сборник. – Москва, 2005. – № 24. – С. 27-38.

[7] Лебедев, А.Н. Вероятностные методы в инженерных задачах: справ. / А.Н. Лебедев, М.С. Куприянов, Д.Д. Недосекин, Е.А. Чернявский. – СПб.: Энергоатомиздат. 2008. – 333 с.

[8] Хан, Г. Статистические модели в инженерных задачах / Г. Хан, С. Шапиро. – М.: Мир, 2010. – 3-е изд. – 412 с.

[9] Вишнівський, В.В. Безконтактний індукційний метод діагностування радіоелектронних блоків : збірник наук. праць ВІКНУ ім. Т. Шевченка / В.В. Вишнівський, М.К. Жердєв, Б.П. Креденцер, В.В, Кузавков. – Київ, 2013. – № 43. – 336 с.

[10] Кузавков, В.В. Діагностична модель p-n (n-p) переходу в динамічному режимі для безконтактного індукційного методу діагностування / М.К. Жердєв / збірник наук. праць ВІКНУ ім. Т. Шевченка. – Київ, 2014. – № 45. – 317 с.

[11] Жердєв, М.К. Узагальнення результатів форсованих випробувань радіоелектронних компонентів / М.К. Жердєв, В.В, Кузавков, І.В. Пампуха / збірник наук. праць ВІКНУ ім. Т. Шевченка. – Київ, 2015. – № 49. – С. 40-47.

[12] Жердєв, М.К. Перевірка адекватності аналітичної моделі радіоелектронного компоненту / М.К. Жердєв, В.В. Кузавков / науковий журнал Інформаційна безпека Східноукраїнський національний університет ім. В. Даля. – Луганськ, 2014. – № 3 (15). – С. 76-81.

[13] Кузавков В. В. Постановка задачі синтезу автономної автоматизованої системи діагностування мережі однотипних програмно-апаратних засобів / В. В. Кузавков, П. В. Хусаїнов, Г. І. Гайдур. // Сучасний захист інформації. – 2017. – №3. – С. 61-67.

[14] Development of object state estimation method in intelligent decision support systems V Bezuhlyi,

V Oliynyk, I Romanenko, O Zhuk, V Kuzavkov, O Borysov, Eastern-European Journal of Enterprise Technologies 5 (3), 113.

APPLICATION OF METHODS OF TECHNICAL DIAGNOSIS IN SOLVING PROBLEMS OF CYBERNETIC PROTECTION

The article substantiates the possibility of using diagnostic information based on physical and chemical processes in semiconductor structures of software and hardware - systems with embedded software of modern telecommunication systems for solving problems of cybernetic protection. The subject of the study is the process of functioning of a set of technical means for receiving, transmitting, storing and processing data in the management of a software component (a set of technical means that are a practical implementation of the OSI model)

A generalized scheme of interaction between the software and hardware components of the selected type of radio-electronic equipment and the features of applying a physical approach to monitoring the technical condition of equipment for solving problems of cyber threats and cyber attacks are given.

The tasks of technical diagnostics include control over changes in the state of the hardware (as a result of aging or replacement) and changes in the software (as a result of failures or interference by unauthorized persons). In any case, the tasks to be solved are related to the assessment of the actual state of the software and hardware, the forecast for the future, the assessment of the probability of failures, the risk of accidents.

Based on the analysis of the values of the diagnostic parameter (in comparison with the reference or calculated values), the place of non-compliance with the established (defined) mode of operation, the causes and possible consequences are established. Decision-making is fundamentally possible in the presence of a diagnostic parameter, the presence of an adequate model of the control object (to obtain calculated data), or a sufficient number of the same type of means with the same operating conditions for statistical processing.

It is proposed to use physical approaches of technical diagnostic methods to solve the following problems: – identification and authentication of telecommunication equipment; definition of atypical load at the program level. The task of improving information security necessitates the search (development) or creation of devices capable of generating electrical signals of a random (noise) nature. The non-contact induction method is considered as the main method.

Keywords: diagnostic parameter, physical and chemical processes, radio-electronic equipment, model, forecasting

Кузавков Василь Вікторович доктор технічних наук, доцент, начальник кафедри Військового інституту телекомунікацій та інформатизації імені Героїв Крут.
E-mail: nevse@ukr.net.
Orcid ID: 0000-0002-0655-9759.

Kuzavkov Vasyl, Doctor of Technical Sciences, Docent, Head of the Department "Construction of Telecommunication Systems" of the Faculty "Telecommunication Systems" of the Military Institute of Telecommunications and Informatization named after the Heroes of Kruty, Kyiv, Ukraine.