УДК 004.056.5
DOI https://doi.org/10.32782/2521-6643-2026-2-72.28

Савченко Ю. В., кандидат технічних наук, доцент,
доцент кафедри кібербезпеки та інформаційних технологій
Університету митної справи та фінансів
ORCID: 0000-0002-7177-6311

Паршина О. А., доктор економічних наук, професор,
професор кафедри кібербезпеки та інформаційних технологій
Університету митної справи та фінансів
ORCID: 0000-0002-7836-0140

Воскобойник В. О., кандидат технічних наук, доцент,
доцентр кафедри інформаційної безпеки та наноелектроніки
Національного університету «Запорізька політехніка»
ORCID: 0000-0003-3786-8666

Корнейко О. В., кандидат технічних наук, професор,
професор кафедри інформаційних технологій та кібербезпеки,
Національної академії внутрішніх справ
ORCID: 0000-0002-1882-9680

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ З ПОЗИЦІЙ СИТУАЦІЙНОГО МЕНЕДЖМЕНТУ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

В статті запропоновано дослідження нових і поліпшення класичних методів і засобів інформаційних систем та технологій передачі повідомлень які додатково посилюють вимоги щодо реалізації високого рівня потенційної захищеності їх штатних тактико-технічних характеристик. Досліджено комплексні системи захисту інформації з позицій ситуаційного менеджменту захищеності в інформаційно-телекомунікаційних системах. Множина складових компонентів об'єкта інформатизації загалом формується як сукупність трьох взаємозалежних підгруп (систем). Вони включають людський фактор, що утворює біосоціальну систему, технічні засоби, їхні системи та приміщення для розміщення, а також комп'ютерно-програмне забезпечення, яке виступає інтелектуальним посередником між людиною й технікою. Гарантування інформаційної безпеки – це безперервний і багатоетапний процес. Він охоплює контроль рівня захищеності інформації, аналіз і усунення вразливих місць у системі захисту, а також розробку і впровадження найбільш ефективних методів модернізації та прогресивних технологічних рішень. У сучасних умовах комплексне використання доступних засобів захисту, зокрема високопрофесійна підготовка користувачів і суворе дотримання ними правил захисту інформації, стають ключовими чинниками забезпечення належного рівня безпеки. Однак важливо пам'ятати, що жодна система захисту не може бути абсолютно бездоганною. Варто зазначити, що всі принципи інформаційної безпеки мають однакову вагу: виділити більш чи менш важливі серед них навряд чи доцільно. Тому в конструкції комплексної системи захисту інформації необхідно розглядати всі принципи як складові одного цілісного механізму, який забезпечує синергетичний ефект. Для підтримки процесів прийняття рішень розроблено структурно-лінгвістичну функціональну схему застосування інформаційно-телекомунікаційних систем. Системи захисту інформації представляють собою організовану сукупність об'єктів і суб'єктів, які реалізують методи і способи захисту за допомогою цілої низки заходів, необхідних для виконання завдань безпеки сучасних інформаційних технологій. Ефективність і надійність таких систем прямо залежить від їхньої збалансованості та комплексного підходу, адже несинхронність між окремими компонентами значно збільшує ризики виникнення «відмов» у роботі. Якість та надійність захисту визначаються не лише різноманітністю складових елементів, але й їхньою повнотою, яку можна досягти при врахуванні всіх актуальних факторів та обставин. Екранування електронно-цифрових пристроїв є необхідною складовою інформаційної безпеки, а застосування технологій безехових камер значно покращує її якість. Усвідомлення важливості комплексного підходу до інформаційного захисту полягає у таких аспектах: інтеграція локальних систем захисту; забезпечення цілісності всієї системи; гарантування всебічного захисту інформації.

Ключові слова: *структурно-лінгвістична функціональна схема, комплексна система захисту інформації, ситуаційний менеджмент, інформаційні системи, службова інформація.*

Savchenko Iu. V., Parshyna O. A., Voskoboinyk V. O., Korneiko O. V. Comprehensive Information Security System Based on Situational Management in Information and Telecommunications Systems

The article proposes research into new and improved classical methods and means of information systems and message transmission technologies, which additionally increase the requirements for implementing a high level of potential security of their standard tactical and technical characteristics. Comprehensive information protection systems are studied from the standpoint of situational security management in information and telecommunication systems. The set of components of an informatization object is generally formed as a set of three interdependent subgroups (systems). They include the human factor, which forms a biosocial system, technical means, their systems and premises for placement, as well as computer software, which acts as an intellectual mediator between man and technology. Ensuring information security is a continuous and multi-stage process. It includes monitoring the level of information security, analyzing and eliminating vulnerabilities in the protection system, as well as developing and implementing the most effective methods of modernization and progressive technological solutions. In modern conditions, the comprehensive use of available protection tools, in particular highly professional training of users and their strict adherence to information protection rules, are becoming key factors in ensuring the proper level of security. However, it is important to remember that no protection system can be absolutely flawless. It is worth noting that all principles of information security have the same weight: it is hardly advisable to single out more or less important ones among them. Therefore, in the design of a comprehensive information protection system, it is necessary to consider all principles as components of a single holistic mechanism that provides a synergistic effect. To support decision-making processes, a structural-linguistic functional scheme for the use of information and telecommunication systems has been developed. Information protection systems are an organized set of objects and subjects that implement methods and means of protection using a whole range of measures necessary to perform security tasks of modern information technologies. The effectiveness and reliability of such systems directly depends on their balance and comprehensive approach, because the asynchrony between individual components significantly increases the risks of «failures» in operation. The quality and reliability of protection are determined not only by the variety of constituent elements, but also by their completeness, which can be achieved by taking into account all relevant factors and circumstances. Shielding of electronic and digital devices is a necessary component of information security, and the use of anechoic chamber technologies significantly improves its quality. Awareness of the importance of a comprehensive approach to information protection consists of the following aspects: integration of local protection systems; ensuring the integrity of the entire system; guaranteeing comprehensive information protection.

Key words: *structural-linguistic functional diagram, complex information protection system, situational management, information systems, official information.*

Постановка проблеми. У сучасному суспільстві, яке постійно зазнає впливу зовнішніх і внутрішніх факторів, серед яких нерідко трапляються недружні, критично важливо ретельно оцінювати всю отримувану інформацію. Адже інформаційні ресурси, засоби і системи передачі, обробки даних, а також всі об'єкти, де встановлені ці засоби та системи – від приміщень до технічного обладнання – можуть бути використані як ефективно, так і з негативними наслідками. Це залежить від заданої інформаційної технології, яка часом може набувати навіть ворожого характеру. Об'єкт інформатизації включає в себе весь спектр інформаційних ресурсів, засобів і систем для обробки даних (що функціонують відповідно до певної інформаційної технології), а також інфраструктуру, приміщення та технічні об'єкти, призначені для роботи цих систем або для ведення конфіденційних переговорів [1, 13, 14].

У даному визначенні ключовим є поняття «сукупність», яке підкреслює, що об'єкт інформатизації являє собою єдину інтегровану інформаційну систему, яка охоплює підприємство, установу чи організацію цілком.

У реальному житті всі елементи об'єктів інформатизації, розміщені в межах одного підприємства чи організації, утворюють єдиний комплекс. Цей комплекс характеризується спільними цілями, завданнями, структурними взаємозв'язками та технологіями інформаційного обміну. Оскільки сучасні підприємства є складними системами, що складаються з різнорідних компонентів, вони здатні змінюватися та адаптуватися у процесі функціонування. Така модифікація часто залежить від взаємодії численних факторів, які складно оцінити кількісно. Особливість складних інформаційних систем полягає в тому, що вони здатні набувати нових властивостей і виходити за межі початкових функцій своїх окремих компонентів. У цьому контексті слід особливо відзначити роль людського фактору: саме вплив людини на кожну підсистему значною мірою визначає функціонування та розвиток таких систем.

Метою статті є дослідження нових і поліпшення класичних методів і засобів інформаційних систем та технологій передачі повідомлень які додатково посилюють вимоги щодо реалізації високого рівня потенційної захищеності їх штатних тактико-технічних характеристик.

Виклад основного матеріалу. Огляд інтегральних компонентів, що складають об'єкт інформатизації. Дійсно, множина компонентів, що складають об'єкт інформатизації, інтегрально представляються у вигляді сукупності трьох підгруп (систем), що складаються з людей (що входять і утворюють біосоціальну систему), техніки, включаючи технічні системи та приміщення, в яких вони розташовані, і відповідне комп'ютерно-програмне забезпечення, що є інтелектуальним посередником між людиною і технікою (що утворюють інтелектуальну систему).

Сукупність цих трьох підгруп утворює соціотехнічну систему. Із самої назви **«соціотехнічна система»** випливає, що вона утворена з наступних підсистем:

– ***соціальної підсистеми***, включаючи зайнятих в організації службовців (їх знання, вміння, настрій, ціннісні установки, ставлення до виконуваних функцій), управлінську структуру і систему заохочень;

– ***технічної підсистеми***, включаючи пристрої, інструменти і технології, що перетворюють вхід у вихід тим способом, який покращує економічну ефективність організації.

Отже створення нових і поліпшення класичних методів і засобів інформаційних систем та технологій передачі повідомлень додатково посилюють вимоги щодо реалізації високого рівня потенційної захищеності їх штатних тактико-технічних характеристик. Однак, навіть завжди апріорна надійність працездатності кібер-фізичних систем – Cyber-Physical Systems (CPS – КФС) [2, с. 34–38] може бути значно змінена не усвідомленими або свідомими діями (атаками) з боку порушників достовірності та цілісності вихідної інформації. При цьому, адресного впливу, на прикладі автоматизованої системи (АС) з КФС, може бути підданий як персонал, так і комплекс засобів її автоматизації (КСА).

Кібер-фізичні системи (КФС) являють собою інтелектуальні комплекси, які об'єднують інтерактивні мережі фізичних та обчислювальних компонентів. Завдяки комп'ютерним мережам і вбудованим контролерам ці системи забезпечують управління фізичними процесами, як автономно, так і за участю людини, через реалізацію механізмів зворотного зв'язку. Наразі кібер-фізичні системи активно впроваджуються у різноманітні сфери людської діяльності, зокрема дослідження космосу, транспортне управління, виробництво, енергетика, військова справа, медицина та створення сучасної інфраструктури. Ключовими елементами для розробки кібер-фізичних систем є засоби вимірювання та їх програмне забезпечення, які використовуються для моніторингу параметрів технологічних процесів і навколишнього середовища. Зазвичай такі системи застосовуються у критичних секторах, тому при їх проектуванні висуваються особливі вимоги до надійності та безпеки. Це забезпечує відповідність високим стандартам щодо оцінки ризиків кібербезпеки, особливо в умовах **принципу невизначеності** [3, 15]. Додатково наголошується на важливості метрологічної достовірності вимірювань, яку гарантують сучасні засоби вимірювання.

Безпосередньо концепція принципу достовірності підтвердження відповідності ЗВ побудована на основі оцінки прийнятних ризиків і аналізу функціонування комбінованої системи підтвердження відповідності в умовах невизначеності, де підсумкові результати вимірів традиційно вимагають наявності їх достовірності, що ототожнюється з їх апостеріорною похибкою. При чому, саме поняття «похибки результату вимірів» корелює з поняттям істинного значення, чого принципово неможливо досягти. Отже, належний метрологічній контроль ЗВ необхідно реалізовувати в умовах невизначеності згідно з міжнародними стандартами, що розробляються відповідно до Директив ISO / МЕК [3].

Проте, досі спостерігається не деяке сприйняття, а часто й протиріччя між традиційним використанням терміну «похибка виміру» і сучасним – «невизначеність виміру», що особливо проявляються при використанні нестандартних засобів вимірювання, які можуть бути і в арсеналі КФС. Фактично з терміном «невизначеність виміру», з'явився цілий напрямок в техніці вимірів, наприклад у радіолокації [4, с. 374], що використовує не стільки нові аналітичні вирази й обчислення, скільки реалізує трансформацію класичного погляду на парадигму вимірювання, обумовлених інтеграційнім процесом міжнародного співтовариства у напрямі гармонізації стандартів и других нормативних документів в області метрології. Саме тому, в ході сучасних подій та явищ безпосередній детальний аналіз радіоелектронних вимірів (як технічної основи КФС) з позицій їх адекватності, достовірності і надійності дозволяє констатувати, що поняття «невизначеність виміру», за відсутності яких ось нових аналітичних виразів і обчислення, відображає деяку трансформацію накопичення знань і досвіду у сфері необхідних умов вимірів, а як достатня умова реалізації достовірності вимірів, – потрібна апостеріорна оцінка у вигляді деякої (наполягаємо, – імовірнісною) міри (сфери) розсіяння результатів виміру. При цьому, до цих результатів доцільно додавати детальні звіти по калібруванню і методам випробувань, які не заперечують міжнародним і національним стандартам і локальним регулюючим державним актам.

Відтак [5], надійність інформаційної системи з поєднанням засобів радіоелектронних вимірів та їхня адекватність і достовірність відповідності у рамках використання принципу невизначеності можна ототожнювати, як з видачою апостеріорних результатів вимірів, так і з виробленням рішення по приписаних їм похибок в можливих інтервалах їх змін у вигляді деяких мереж (сфер) розходження, що безпосередньо і буде відображати наявність обліку факту невизначеності вимірів. При цьому невизначеність проявів ризиків завжди присутній при будь-якому прийнятті рішень (виборі) з оцінки (недооцінки / переоцінці) важливості інформації і потенційних для неї загроз. Тому ІС, засоби захисту інформації (ЗЗІ) та процес оптимізації їх використання в залежності від співвідношення потенційних загроз і можливостей знищування них підлягають захисту и апріорі потребують серйозних економічних витрат. Величина таких витрат зазвичай визначається на фоні невизначеності як при розділені інформаційних ресурсів на категорії, так і ЗЗІ по їх цінності при оцінюванні еквівалентної вартості експлуатації самих засобів, не виключаючи заходи щодо запобігання атак на них, наприклад, в процесі використання їх побічних електромагнітних випромінювань і наводок [6, 7].

Сучасне підприємство, яке забезпечує захист інформації, являє собою складну багатофакторну систему з характерними особливостями. Серед них – багаторівнева організаційна структура, багатогранність функціональних процесів, високий рівень технічного забезпечення, численні кооперацiйні зв'язки, необхідність розширеного доступу до інформації та зростаюча роль безпаперових технологій в обробці даних. Також варто відзначити збільшення частки автоматизованих процедур у загальному обсязі обробки інформації, важливість прийняття рішень на основі автоматизованих даних, високу концентрацію інформаційних ресурсів в автоматизованих системах та їхню територіальну розподіленість.

Крім того, підприємства стикаються з такими викликами, як акумулювання значних обсягів даних на технічних носіях, інтеграція різнорідної інформації в єдині бази даних, довготривале зберігання великих обсягів машинної інформації, забезпечення одночасного доступу різним категоріям користувачів до ресурсів. При цьому відзначається активна циркуляція інформації між компонентами автоматизованих систем, у тому числі віддаленими.

Реалізація індустрії обробки інформації сприяє підвищенню продуктивності праці та покращенню умов життя людини. Водночас вона створює низку серйозних і масштабних проблем, які потребують вирішення в умовах зростаючої цифровізації та автоматизації процесів.

Структурно-лінгвістична функціональна схема (СЛФС). Одним із ключових завдань є забезпечення збереження та визначеного статусу інформації, яка циркулює та обробляється на підприємстві. Для цього необхідно створити комплексну систему захисту інформації, яка має відповідати таким вимогам:

– Бути узгодженою з цілями та завданнями захисту інформації на конкретному підприємстві.

– Забезпечувати цілісність, охоплюючи всі складові з чіткими структурними зв'язками між елементами, що гарантують її гармонійне функціонування.

– Бути всеосяжною, враховуючи всі об'єкти захисту, їх компоненти, вплив різних обставин та факторів на безпеку інформації, а також охоплювати всі методи та засоби захисту.

– Мати достатній рівень надійності для виконання покладених завдань і забезпечувати стабільний результат завдяки високій якості всіх складових системи.

– Органічно інтегруватися у технологічні процеси збору, зберігання, обробки, передачі та використання інформації.

– Бути логічно, технологічно та економічно обґрунтованою.

– Можливість реалізації завдяки забезпеченню необхідними ресурсами.

– Відзначатися простотою та зручністю в експлуатації, управлінні і використанні законними користувачами.

– Функціонувати безперервно і бути гнучкою, здатною адаптуватися до змін умов, технологій обробки даних та елементів системи.

Така система захисту має гарантувати стабільність і безпеку інформаційного середовища підприємства.

Основним напрямком пошуку нових способів захисту інформації є не просто розробка відповідних механізмів, а впровадження систематичного процесу, який охоплює всі етапи життєвого циклу інформаційних систем. Цей процес має включати комплексне використання доступних засобів захисту, які в найбільш ефективний спосіб об'єднуються в єдиний цілісний механізм. Завдання полягає у створенні захисту не лише від зловмисників, але й від некомпетентності або недостатньої підготовленості користувачів і персоналу, а також нештатних технічних ситуацій.

Головна проблема впровадження систем захисту полягає в забезпеченні надійної охорони самої інфраструктури отримання, обробки та зберігання даних. Критично важливо виключити будь-яке випадкове або навмисне отримання інформації сторонніми особами завдяки обмеженню або навіть повній забороні доступу до пристроїв та ресурсів інформаційних систем для всіх без винятку користувачів, включаючи адміністрацію та технічний персонал. Водночас системи захисту повинні бути спроектовані так, щоб не ускладнювати роботу користувачів із ресурсами системи.

Забезпечення необхідного рівня захисту інформації є складною задачею, яка вимагає не лише реалізації певного набору наукових, технічних і організаційних заходів, а й розробки цілісної системи організаційно-технологічних рішень із застосуванням спеціалізованих методів і засобів. Підхід до вирішення цієї проблеми повинен бути комплексним і враховувати всі аспекти захисту інформації.

На основі теоретичних досліджень і практичного досвіду в галузі інформаційної безпеки розроблено системно-концептуальний підхід до її забезпечення. Цей підхід спрямований на створення єдиної політики, яка базується на науково обґрунтованих принципах і рішеннях, достатніх для ефективної організації захисту інформації та забезпечення її надійності. Основна мета такого підходу полягає в систематизації й координації всіх дій, спрямованих на побудову безпечного інформаційного середовища.

Системний підхід передбачає кілька важливих аспектів. По-перше, це цільова системність, коли захищеність інформації розглядається як невід'ємна складова загального визначення її якості. По-друге, просторовий аспект, який забезпечує вирішення питань захисту у всіх підрозділах та структурах компанії. По-третє, тимчасова системність гарантує безперервність заходів із захисту інформації відповідно до

регламентів і стратегії підприємства. Нарешті, організаційна системність забезпечує єдність управління та координації всіх процесів, пов'язаних із інформаційною безпекою.

Комплексний системний підхід до створення будь-якої системи охоплює ретельний аналіз та врахування низки критичних аспектів. Перш за все, здійснюється вивчення об'єкта, для якого впроваджується система, та оцінка потенційних загроз його безпеці. Далі проводиться аналіз ресурсів, необхідних для побудови системи, оцінка її економічної доцільності, а також детальне дослідження самої системи: її властивостей, принципів функціонування та способів підвищення ефективності. Особлива увага приділяється співвідношенню внутрішніх і зовнішніх факторів, а також можливості внесення додаткових змін на всіх етапах створення системи, забезпечуючи організованість процесу від початку до завершення.

Загалом, системний підхід – це методологія аналізу проєктів, що передбачає розгляд системи як єдиного цілого, а не окремих її частин. Основна мета такого підходу полягає в оптимізації функціонування всієї системи загалом, а не точковому покращенні окремих елементів. Це особливо важливо через ризик того, що покращення одного параметра може негативно вплинути на інші. Тому головним завданням є досягнення балансу між суперечливими вимогами та характеристиками для забезпечення гармонійного функціонування системи.

Комплексний (системний) підхід передбачає, що створення будь-якої системи має початися лише після чіткого визначення її основних компонентів:

– Вхідні елементи. Це ті дані чи фактори, з якими буде працювати система. У контексті безпеки, наприклад, до вхідних елементів відносяться потенційні загрози, які можуть виникати на конкретному об'єкті.

– Ресурси. Система потребує певних засобів для свого запуску та функціонування. Сюди входять матеріальні витрати, енергоспоживання та інші необхідні ресурси.

– Параметри навколишнього середовища. Система завжди взаємодіє з іншими системами чи об'єктами навколо неї. Важливо окреслити межі цієї взаємодії, зокрема визначити сфери відповідальності підприємства, яке реалізує систему. Наприклад, захист інформації, що передається через лінії зв'язку між об'єктами, потребує чіткого розподілу функцій безпеки. Взаємодію з навколишнім середовищем і межі системи ігнорувати не можна, адже це може призвести до неефективності прийнятих рішень.

– Цільове призначення і функції. Для кожної системи слід визначити її мету або функціональне призначення, до якого вона має прагнути. Чіткість і конкретність формулювання цих цілей дозволить вибрати найефективніше рішення для побудови системи. Якщо вдатися до загальних формулювань мети, наприклад «забезпечення безпеки об'єкта», то це може потребувати розробки глобальної системи захисту. Якщо ж мета буде визначена детальніше – як, наприклад, «забезпечення безпеки передачі інформації всередині будівлі», то коло можливих рішень суттєво звузиться. Реалізація загальної цілі часто передбачає досягнення кількох локальних цілей через побудову так званого «дерева цілей», що спрощує та здешевлює створення системи.

– Критерії ефективності. Вибір напрямків побудови системи базується на її здатності забезпечувати визначені цілі. Критерії ефективності слугують інструментом для оцінки якості виконання функцій системи, враховуючи витрати ресурсів. Такий інструмент має бути ясним, однозначним і дозволяти кількісну оцінку характеристик системи на всіх етапах її розробки та експлуатації. Ця структура забезпечує комплексний підхід до створення системи, враховуючи всі найважливіші аспекти її функціонування та взаємодії з оточенням.

Для забезпечення успішного захисту службової інформації на підприємстві, особливо в умовах дефіциту часу та різноманіття потенційних загроз (внутрішніх і зовнішніх), необхідно створити сучасні, надійні засоби захисту інформації. Складність структур підприємств та фактор людського втручання в технологічні процеси обробки інформації ще більше ускладнюють це завдання. Тому найоптимальнішим підходом стає впровадження комплексної системи захисту, що базується на безперервному циклі з кількох основних етапів:

1. Визначення інформації, яка потребує захисту.

2. Проведення оцінки вразливості й ризиків для визначеної інформації через існуючу сукупність загроз і можливих каналів витоку.

3. Ідентифікація й аналіз потенційних загроз і каналів витоку інформації, а також встановлення вимог до системи захисту.

4. Вибір відповідних засобів захисту та визначення їхніх технічних характеристик.

5. Впровадження та організація застосування обраних заходів і засобів захисту.

6. Контроль цілісності системи й управління її функціонуванням. Кожен з цих етапів сприяє формуванню уточнених вимог, необхідних для модернізації засобів захисту інформації.

Це дозволяє досягати синергетичного ефекту в сфері логістики, управління і підвищення конкурентоспроможності підприємств різного профілю діяльності. Як зазначалося раніше, із позицій отримання позитивного синергетичного ефекту у сфері управління підприємствами, особливо у випадках диверсифікації, створення концернів або кооперацій, не можна ігнорувати питання безпеки інформаційного середовища. Це стає особливо актуальним для об'єктів критичної інфраструктури, які потребують впровадження комплексної системи захисту інформації. Реалізація таких систем, з урахуванням новітніх інформаційних технологій та інтеграції критично важливих ресурсів підприємства, має враховувати внутрішні й зовнішні фактори

впливу на стабільне функціонування об'єкта. При цьому, на таких об'єктів реалізація системи управління з новітніми інформаційними технології, навіть за наявністю власної критичної інформаційної інфраструктури (КІІ), не може формуватися відірвано від внутрішніх та зовнішніх чинників впливу на штатний режим їх життєдіяльності», де процеси інформаційної підтримки прийняття рішень відображені на рис. 1 (адаптовано згідно [8], с. 23) з використанням інформаційно-телекомунікаційної системи (ІТС)

Таким чином, системи захисту інформації – це організована сукупність об'єктів і суб'єктів ЗІ, що забезпечує реалізацію способів і методів, здійснюваних засобами захисних заходів для вирішення завдань безпеки сучасних інформаційних технологій. При цьому компоненти ЗІ, з одного боку, є складовою частиною системи, а з іншого – самі організовують систему, здійснюючи захисні заходи. Оскільки система може бути визначена як сукупність взаємопов'язаних елементів, то призначення ЗЗІ полягає в тому, щоб об'єднати всі складові захисту в єдине ціле, в якому кожен компонент, виконуючи свою функцію, одночасно забезпечує виконання функцій іншими компонентами і пов'язаний з ними логічно і технологічно шляхом отримання синергетичного ефекту.

Слід мати на увазі, що працездатність, а, отже, і надійність захисту інформації прямо пропорційна системності та її комплексності, так як при неузгодженості між собою окремих складових частота «відмов» в технології захисту збільшується. При цьому необхідність комплексності рішень полягає перш за все в об'єднанні в єдине ціле локальних (правових, організаційних, інженерно-технічних і т. п.) ЗЗІ з оптимально корельованими логічними і технологічними всіх реалізованих складових захисту.

Рис. 1. СЛФС процесів інформаційної підтримки прийняття рішень з використанням ІТС

Звідси якість і надійність захисту залежать не тільки від видів складових системи, але і від їх повноти, яка забезпечується при врахуванні всіх факторів і обставин, що впливають на захист. Саме повнота всіх складових системи захисту, що базується на аналізі таких факторів і обставин, є другим призначенням комплексності.

У 21 столітті, коли електронно-цифрові прилади стали невід'ємною частиною нашого повсякденного життя, надзвичайно актуальним є питання інформаційної безпеки, особливо щодо мінімізації ризиків і наслідків атак різного походження – як зовнішніх, так і внутрішніх. Одним із методів таких атак є «атаки через сторонні канали зв'язку», спрямовані на ураження цифрових пристроїв. Сутність таких атак полягає у використанні інформації, яка генерується у вигляді фізичних процесів у пристроях, але не враховується в їхньому теоретичному функціонуванні. Такі атаки створюють фізичний вплив на електронно-цифрову техніку або мережі, що до неї підключені. Прикладом є атаки через електромагнітне випромінювання, які класифікуються як пасивні. У цьому випадку електронні шифрувальні пристрої під час роботи виділяють електромагнітне випромінювання. Аналізуючи певні спектральні компоненти цього випромінювання, можна отримати цінну інформацію, зокрема, визначити секретний ключ шифрування або самі дані, які обробляються. Окрім цього, варто враховувати і електромагнітні перешкоди – небажані впливи, що виникають через взаємодію електричних, магнітних або електромагнітних полів із технічними пристроями. Це може призводити до погіршення їхньої роботи або змін характеристик [9]. Для протидії таким загрозам застосовують різноманітні методи захисту. Один із найпростіших та ефективних способів – використання екранування корпусу електронного пристрою, наприклад комп'ютера чи сервера. Екранування значно зменшує ймовірність впливу атак шляхом блокування побічного електромагнітного випромінювання та наведень (ПЕВН), що може зменшити ризик витоку інформації.

Однак, традиційне екранування іноді може бути недостатньо ефективним для забезпечення необхідного рівня захисту. У таких випадках доцільно застосовувати безехові камери (БЕК). Замість звичайного корпусу комп'ютерні комплектуючі можуть встановлюватися в спеціально розроблений «модернізований

корпус», який функціонує за принципом безехової камери. Такий підхід дозволяє значно знизити ризики ненавмисного витоку інформації. Крім того, серверні приміщення також можуть бути оснащені безеховими камерами для забезпечення максимального рівня безпеки й захисту від шкідливих впливів.

Значимість комплексного підходу щодо захисту інформації. Найпростішим прикладом радіочастотної камери є звичайна екранована конструкція, створена за принципом клітки Фарадея. Вона являє собою герметичний об'єм, зібраний із модульних конструкцій (раніше такі камери робили зі зварних елементів), який забезпечує захист секретної інформації шляхом перекриття радіочастотного каналу. Головна функція цих камер полягає у фільтрації та усуненні небажаних перешкод у живленні. Радіосигнали у такій камері не здатні проникнути ані ззовні всередину, ані навпаки. Подібні технології знаходять застосування як для захисту електронних і цифрових пристроїв від зовнішніх впливів, так і для запобігання внутрішньому й зовнішньому прослуховуванню. Наприклад, можна використати рупороподібну безехову камеру (БЕК), стінки якої, основне джерело паразитних відбиттів, вкриті радіопоглинаючим матеріалом (РПМ), таким як В2-Ф3 з коефіцієнтом відбиття по потужності Kn = 0,05 (–13 дБ), основою якого служить фольгований склопластик. Додатково цей матеріал сприяє екрануванню. Згідно з даними досліджень, при довжині хвилі $\lambda = 4{,}3$ см коефіцієнт безлунності (КБЕ) камери становить –47 дБ, а при $\lambda = 3$ см – –50 дБ. Для інших ділянок робочого спектра значення КБЕ залишалося на рівні не гірше –35 дБ. Таким чином, БЕК створює контрольоване середовище, яке надійно запобігає перехопленню інформації [15].

Отже, можна зробити висновок, що екранування електронно-цифрових пристроїв, зокрема персональних комп'ютерів, є ключовим компонентом забезпечення інформаційної безпеки загалом. Використання технологій безехових камер суттєво покращує рівень захисту інформації. Проте важливо брати до уваги всі параметри уразливості інформації та потенційні загрози її безпеці, охоплювати усі об'єкти захисту, застосовувати різноманітні методи і засоби захисту, гарантувати безпеку працівників і впроваджувати заходи відповідно до цілей та завдань захисту. Тільки комплексний підхід здатний забезпечити безпеку всієї інформації незалежно від умов. Це означає, що захищенню підлягають усі носії інформації та всі етапи її збору, зберігання, передачі й використання за будь-яких режимів функціонування системи обробки даних. Дотримання комплексного підходу, водночас, не виключає необхідності диференційованого захисту залежно від типу носіїв інформації, її секретності, засобів зберігання і обробки, а також можливих форм вразливостей та шляхів несанкціонованого доступу. Тому важливість комплексного підходу полягає у забезпеченні інтеграції локальних систем захисту, повноти всіх елементів системи та всебічності захисту інформації. З огляду на це, можна стверджувати, що комплексна система захисту інформації охоплює всі аспекти діяльності людини, аби гарантувати безпечне отримання, обробку, використання та зберігання даних, які потребують захисту.

При побудові будь-якої комплексної системи захисту інформації необхідно заздалегідь обумовлювати принципи її побудови. Як правило, КСЗІ – це складна система, яка функціонує ***в умовах невизначеності*** у сфері ***ситуаційного менеджменту*** (див. рис. 2) та вимагає значних матеріальних витрат.

Зокрема, поняття ***невизначеності*** широко використовується в галузях освіти, науки, техніки та інших сферах життєдіяльності соціуму. Так, для забезпеченні метрологічної достовірності вимірювань за допомогою штатних засобів вимірювання предусмотрені навіть нормативні світові стандарти в виде ISO/IEC Guide 98-1:2009 [3]. В квантовой фізиці використовують ***принцип невизначеності*** Гейзенберга [10], в вигляді фундаментальної концепції, яка стверджує, що неможливо одночасно знати точне положення та імпульс елементарної частинки, що виникає через частинково-хвильовий дуалізм таких частинок у квантовій механіці. Це означає, що елементарні частинки можуть поводитися і як хвилі, і як частинки залежно від обставин. При цьому, одним із ключових наслідків цього принципу невизначеності, є обмеження того, наскільки точно ми можемо виміряти властивості таких елементарних частинок.

Ситуаційний менеджмент [11] у процесі прийняття управлінських рішень в умовах глобалізації, цифрових технологій, економічних криз та інформаційних викликів діє як один із найефективніших підходів. Ця концепція базується на здатності оперативно ухвалювати рішення, зважаючи на конкретні обставини та особливості кожної ситуації. У сучасному світі, де розвиток технологій і зростання непередбачуваних загроз значно впливають на соціальні та економічні процеси, ситуаційний менеджмент забезпечує керівникам інструменти для швидкого аналізу ситуації та прийняття ефективних рішень. Завдяки своїй гнучкості цей підхід дозволяє різним управлінським ланкам оперативно діяти у змінних умовах, наприклад, у бізнес-середовищі або під час сценаріїв мережоцентричних конфліктів, реалізуючи при цьому відповідні концептуальні моделі. Принципи ситуаційного менеджменту, такі як класифікація управлінських ситуацій, аналіз і застосування релевантних методів оцінки, мають важливе значення для зміцнення безпеки та конкурентоспроможності підприємств. Слід зазначити, що найбільшу роль у його ефективності відіграють гнучкість, інноваційність і здатність адаптувати рішення до нових викликів у кризових умовах. У зв'язку з цим якісне визначення ключових принципів побудови комплексної системи захисту інформації (КСЗІ) залишається актуальним завданням, яке потребує професійного підходу. Зокрема, увага має бути зосереджена на таких основних принципах:

1) Принцип законності: заходи з інформаційної безпеки повинні відповідати чинному законодавству країни щодо захисту інформації. У разі відсутності необхідних законів слід опиратися на інші нормативно-правові акти, які регулюють сферу захисту інформації.

2) Принцип повноти захисту інформації: це стосується захисту не лише державної, комерційної або службової таємниці, але й іншої несекретної інформації, втрата якої може спричинити шкоду її власникам. Впровадження цього принципу також гарантує охорону інтелектуальної власності.

3) Принцип обґрунтованості захисту: передбачає проведення експертної оцінки щодо доцільності засекречування певної інформації, враховуючи економічні чи інші потенційні наслідки. Це дозволяє ефективно використовувати ресурси лише на ті аспекти захисту, які є критично важливими.

4) Принцип створення спеціалізованих підрозділів: комплексний захист можливий лише за рахунок формування відповідальних структур, здатних проєктувати ефективні заходи і забезпечувати їх виконання.

5) Принцип залучення всіх залучених осіб: кожен співробітник, який контактує з інформацією, зобов'язаний брати участь у її захисті. Такий підхід сприяє посиленню загального рівня інформаційної безпеки. Дотримання цих принципів дозволяє створити ефективну систему захисту інформації та забезпечити належну реакцію на виклики сучасного світу.

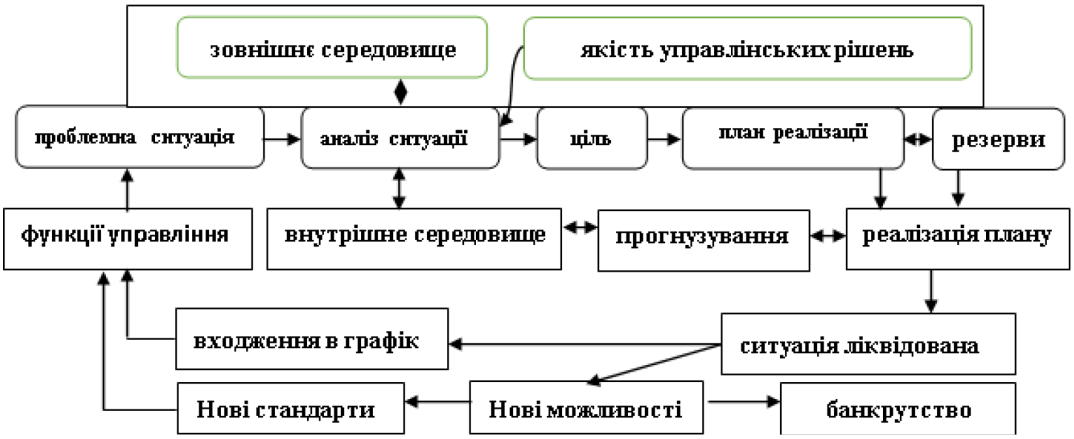

Рис. 2. Концептуальна модель ситуаційного менеджменту – адаптована з [11]

6) Принцип участі всіх дотичних до інформації осіб у її захисті, адже збереження та нерозголошення даних є службовим обов'язком кожного, хто за характером своєї роботи має доступ до захищеної інформації. Така колективна участь сприяє покращенню ефективності заходів із захисту.

7) Принцип персональної відповідальності, який передбачає, що кожна особа несе індивідуальну відповідальність за збереження довіреної їй інформації. У разі втрати або розголошення захищених даних передбачено кримінальну, адміністративну чи іншу відповідальність за правопорушення.

8) Принцип використання необхідних правил і засобів, який вимагає комплексного підходу до побудови КСЗІ. Зокрема, це передбачає залучення керівництва підприємства, спеціалізованих служб захисту та всіх співробітників, які працюють з інформацією. Додатково акцентується увага на застосуванні різних організаційних методів та наявності достатніх матеріально-технічних ресурсів, включаючи технічні засоби захисту.

9) Принцип превентивності передбачає впровадження заходів захисту на випередження – ще до початку розробки чи отримання інформації. Відповідно до цього принципу, особливо важливим є створення заздалегідь захищених інформаційних технологій.

Слід зауважити, що серед розглянутих принципів неможливо виділити важливіші чи менш важливі. Тому в побудові КСЗІ доцільно використовувати всі принципи в комплексі, щоб досягти їхнього синергетичного ефекту.

Висновки. Забезпечення інформаційної безпеки є безперервним процесом, що включає контроль за її захищеністю, виявлення слабких місць у системі захисту, а також обґрунтування і впровадження оптимальних рішень для модернізації та використання передових технологій. В умовах сучасного світу повноцінна безпека інформації досягається лише за умов комплексного застосування всіх доступних засобів захисту, які передбачають не лише технічні рішення, але й високий рівень підготовки користувачів та чітке дотримання ними правил безпеки. При цьому важливо пам'ятати, що абсолютно надійної системи захисту не існує. Варто також підкреслити, що серед основних принципів побудови комплексної системи захисту інформації неможливо визначити більш або менш важливі; ефективність забезпечення цієї безпеки залежить від їхнього спільного використання, яке забезпечує синергетичний ефект. Надійність роботи системи захисту перебуває у прямій залежності від її цілісності й системності, адже будь-які недоліки або невідповідності між окремими компонентами збільшують ризик виникнення збоїв у технології захисту. Окрім того, якість і надійність системи прямо залежать не лише від її складових, але й від їхньої повноти, яка забезпечується

врахуванням усіх факторів та умов, що впливають на безпеку. Екранування електронно-цифрових пристроїв, зокрема комп'ютерів, є невід'ємною складовою інформаційної безпеки. Крім цього, використання технологій безехових камер значно підвищує рівень захисту. Важливість комплексного підходу полягає у забезпеченні взаємозв'язку між локальними системами захисту, у реалізації повноти всіх компонентів системи та досягненні всеосяжності захисту інформації.

Список використаних джерел:

1. Інформаційна безпека підприємства: Навчальний посібник / Н. В. Гришина. – 2-е изд., доп. – М. : Форум: НИЦ ИНФРА-М, 2015. 240 с.

2. Кіберфізичні системи та їх програмне забезпечення / Ван Чунжі, С. П. Яцишин, О. В. Лиса, А.-В. В. Мідик (2018). Вимірювальна техніка та метрологія: міжвідомчий науково-технічний збірник. Львів: Видавництво Львівської політехніки. Том 79. № 1. С. 34–38.

3. ISO/IEC Guide 98-1:2009, Uncertainty of measurement – Part 1: Introduction to the expression of uncertainty in measurement, IDT. Невизначеність виміру. Частина 1. Введення в посібники з виразу невизначеності виміру. М. Стандартінформ. 2017.

4. Тарасенко Ю. С. Фізичні основи радіолокації. Дніпро: Пороги. 2011. 487 с

5. Тарасенко Ю. С., Соляніков В.Г. Інформаційні системи з позицій забезпечення надійності та невизначеності вимірювань. Збірник матеріалів міжнародної науково-практичної інтернет-конференції «Інноваційні технології, моделі управління кібербезпекою – «ІТМК-2021», Дніпро, 14 – 16 квітня 2021 р. 2021. с. 29–30

6. Ю. С. Тарасенко, Д. С. Кузьменко. Щодо оцінки ефективності засобів захисту інформації. Матеріали міжнародної наукової конференції «Математичні проблеми технічної механіки та прикладної математики». Інноваційні технології, прогнозування та моделювання в соціальній сфері, економіці. Моделі корпоративного управління кібербезпекою – Дніпро, Кам'янське. 2019.(2). С. 72–73

7. Кірєєва Н. В., Семенов А. В. Витік інформації по каналах ПЕМІ та способи їх захисту. *Міжнародний журнал прикладних та фундаментальних досліджень*. 2016. № 8–4. С. 499–504.

8. Завгородня Г. А. Інформаційна система підвищення надійності потенційно небезпечних об'єктів. С. 23–24. Міжнародна наукова інтернет-конференція «Інформаційне суспільство:технологічні, економічні та технічні аспекти становлення (випуск 41)» / Збірник тез доповідей: випуск 41 (м. Тернопіль, 13 вересня 2019 р.). Тернопіль. 2019. 100 с.

9. Кузьменко Д. С., Луценко В. В., Тарасенко Ю. С. (2018) Питання підвищення рівня захищеності в інформаційно-телекомунікаційних системах. С. 71–73. Комп'ютерна інженерія і кібербезпека : досягнення та інновації : матеріали Всеукр. Наук.-практ. Конф. Здобувачів вищої освіти й молодих учених (м. Кропивницький, 27–29 листоп. 2018 р.)

10. Величко С. П., Костенко Л. Д. Вивчення основ квантової фізики: Навчальний посібник для студентів вищих навчальних закладів. – Кіровоград : РВЦ КДПУ ім. В. Винниченка, 2002. 274 с.

11. Бондар О. В. Ситуаційний менеджмент. Навч. посіб. Київ : Центр учбової літератури, 2012. 388 с.

12. Козіна Г. Л., Савченко Ю. В., Воскобойник В. О, Прокопович-Ткаченко Д. І., Кацюба В. В. Математичний підхід до підвищення швидкодії програмної реалізації криптоалгоритму SM4. *Системи та технології*, 68 (2). С. 78–85. DOI https://doi.org/10.32782/2521-6643-2024-2-68.9

13. V. Voskoboinyk, Iu. Savchenko, L. Karpukov, O. Parshyna, Prokopovych-Tkachenko D. I. Assessment of the state of information security using expert systems. Systems and Technologies, 2024. 67 (1). С. 72–79 DOI: 10.32782/2521-6643-2024-1-67.11

14. Тарасенко Ю. С., Савченко Ю.В. Ризик-орієнтовані процеси забезпечення безпеки об'єктів критичної інфраструктури. *Системи та технології*, 2023. 65 (1). С. 66–76. DOI https://doi.org/10.32782/2521-6643-2023.1-65.9

15. Тарасенко Ю. С., Прокопович-Ткаченко Д. І., Савченко Ю. В., Воскобойник В. О. Радіоелектронних вимірювань: від погрішності до невизначеності. *Системи та технології*, 2020. 60 (2). С. 102–119. DOI: https://doi.org/10.32836/2521-6643-2020.2-60.7

References:

1. Informatsiyna bezpeka pidpryyemstva: Navchal′nyy posibnyk / N. V. Hryshyna. – 2-e yzd., dop. – M. : Forum: NYTS YNFRA-M, 2015. – 240 s.

2. Van Chunzhi, S. P. Yatsyshyn, O. V. Lysa, A.-V. V. Midyk. (2018). Kiberfizychni systemy ta yikh prohramne zabezpechennya. Vymiryuval′na tekhnika ta metrolohiya: mizhvidomchyy naukovo-tekhnichnyy zbirnyk. L′viv: Vydavnytstvo L′vivs′koyi politekhniky, 2018. Tom 79. № 1. S. 34–38.

3. ISO/IEC Guide 98-1:2009, Uncertainty of measurement – Part 1: Introduction to the expression of uncertainty in measurement, IDT. Nevyznachenist′ vymiru. Chastyna 1. Vvedennya v posibnyky z vyrazu nevyznachenosti vymiru. M. Standartinform. 2017.

4. Tarasenko, Y.S. (2011). Fizychni osnovy radiolokatsiyi. Dnipro : Porohy, 487 s

5. Tarasenko, Y. S., Solyannikov V. H. (2021). Informatsiyni systemy z pozytsiy zabezpechennya nadiynosti ta nevyznachenosti vymiryuvan′. Zbirnyk materialiv mizhnarodnoyi naukovo-praktychnoyi internet-konferentsiyi «Innovatsiyni tekhnolohiyi, modeli upravlinnya kiberbezpekoyu – «ITMK-2021», Dnipro, 14–16 kvitnya 2021 r. s. 29–30

6. Yu. S. Tarasenko, D. S. Kuz′menko. (2019). Shchodo otsinky efektyvnosti zasobiv zakhystu informatsiyi. Materialy mizhnarodnoyi naukovoyi konferentsiyi «Matematychni problemy tekhnichnoyi mekhaniky ta prykladnoyi matematyky». Innovatsiyni tekhnolohiyi, prohnozuvannya ta modelyuvannya v sotsial′niy sferi, ekonomitsi. Modeli korporatyvnoho upravlinnya kiberbezpekoyu/ – Dnipro, Kam'yans'ke – 2019(2). S. 72–73

7. Kiryeyeva, N. V., Semenov, A. V. (2016). Vytik informatsiyi po kanalakh PEMI ta sposoby yikh zakhystu. *Mizhnarodnyy zhurnal prykladnykh ta fundamental'nykh doslidzhen'*. 2016. № 8–4. S. 499–504.

8. Zavhorodnya, H. A. (2019). Informatsiyna systema pidvyshchennya nadiynosti potentsiyno nebezpechnykh ob'yektiv. S. 23–24. Mizhnarodna naukova internet-konferentsiya "Informatsiyne suspil'stvo: tekhnolohichni, ekonomichni ta tekhnichni aspekty stanovlennya (vypusk 41)" / Zbirnyk tez dopovidey: vypusk 41 (m. Ternopil', 13 veresnya 2019 r.). Ternopil'. 2019. 100 s.

9. Kuz′menko, D. S., Lutsenko, V. V., Tarasenko, Y. S. (2018). Pytannya pidvyshchennya rivnya zakhyshchenosti v informatsiyno-telekomunikatsiynykh systemakh. S. 71–73. Komp'yuterna inzheneriya i kiberbezpeka: dosyahnennya ta innovatsiyi: materialy Vseukr. Nauk.-prakt. Konf. Zdobuvachiv vyshchoyi osvity y molodykh uchenykh (m. Kropyvnyts′kyy, 27–29 lystop. 2018 r.)

10. Velychko, S. P., Kostenko, L. D. (2002). Vyvchennya osnov kvantovoyi fizyky: Navchal′nyy posibnyk dlya studentiv vyshchykh navchal′nykh zakladiv. – Kirovohrad : RVTS KDPU im. V. Vynnychenka, 274 s.

11. Bondar, O. V. (2012). Sytuatsiynyy menedzhment. Navch. posib. Kyyiv : Tsentr uchbovoyi literatury. 388 s.

12. Kozina, H. L., Savchenko, Yu. V., Voskoboynyk, V. O, Prokopovych-Tkachenko D. I., Katsyuba V. V. (2024). MATEMATYCHNYY PIDKHID DO PIDVYSHCHENNYA SHVYDKODIYI PROHRAMNOYI REALIZATSIYI KRYPTOALHORYTMU SM4. Systemy ta tekhnolohiyi, 68 (2). S. 78–85. DOI https://doi.org/10.32782/2521-6643-2024-2-68.9

13. V. Voskoboinyk, Iu. Savchenko, L. Karpukov, O. Parshyna, Prokopovych-Tkachenko D. I. (2024). Assessment of the state of information security using expert systems. Systems and Technologies, 67 (1). S. 72–79 DOI: 10.32782/2521-6643-2024-1-67.11

14. Tarasenko, Yu. S., Savchenko, Yu.V. (2023). Ryzyk-oriyentovani protsesy zabezpechennya bezpeky ob″yektiv krytychnoyi infrastruktury. Systemy ta tekhnolohiyi, 65 (1). S. 66–76. DOI https://doi.org/10.32782/2521-6643-2023.1-65.9

15. Tarasenko Yu. S., Prokopovych-Tkachenko D. I., Savchenko Yu. V., Voskoboynyk V. O. (2020). Radioelektronnykh vymiryuvan′: vid pohrishnosti do nevyznachenosti. Systemy ta tekhnolohiyi, 60 (2). S. 102–119. DOI: https://doi.org/10.32836/2521-6643-2020.2-60.7

Дата першого надходження статті до видання: 21.03.2026
Дата прийняття статті до друку після рецензування: 17.04.2026
Дата публікації (оприлюднення) статті: 30.05.2026