УДК 621.391 DOI: 10.26565/2519-2310-2022-1-05

ОСОБЛИВОСТІ ІНТЕГРАЦІЇ СИСТЕМ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНИХ ДІЙ В СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Ольга Мелкозьорова, Юлія Лєсная, Сергій Малахов

Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
olha.melkozerova@karazin.ua, xa12284109@student.karazin.ua, mailgate@meta.ua

Надійшла: червень 2022. Прийнята: серпень 2022.

Анотація: *Метою даного матеріалу є стислий розгляд основних варіантів інтеграції елементів систем (підсистем) захисту від несанкціонованих дій (НСД) до складу інформаційних систем різного призначення. Відзначено, що ступінь і спосіб взаємної інтеграції основних систем (базової системи (тієї, що захищається) та, власне системи/підсистеми захисту) є наслідком проекції реалізованих ієрархічних відносин між ними. Звернено особливу увагу на те, що залежно від умов експлуатації і цільового призначення базової системи, можлива значна ре конфігурація логіки їх взаємовідносин у частині глибини взаємного контролю та можливостей блокування заданих функцій управління (критичних процедур або процесів). Підкреслено, що при загальній схожості базових ідей та цільових установок, особливості проектування підсистем (засобів) захисту від НСД, у кожному конкретному випадку мають свою яскраво виражену специфіку та обмеження. Акцентовано увагу на те, що заявлений рівень легітимації основних процедур управління визначає потрібний рівень інтеграції відповідних систем (систем, котрі поєднуються). Зроблено висновок, що рівень функціональної залежності підсистеми захисту від НСД, від поточних режимів роботи базової системи та дій персоналу, визначається переліком і змістом покладених на неї задач.*

Ключові слова: *інформаційні системи; делегування повноважень; ланки управління; сумісні дії; санкціонування;НСД; інформаційна безпека.*

1. Вступ

У ході розробки та модернізації інформаційних систем (ІС) різного призначення, котрі забезпечують виконанні особливо відповідальних технологічних процедур і процесів, питання щодо підтримки заданого рівня контролю та безпеки реалізації найбільш значущих *(критичних*) процедур управління є найбільш принциповими. Як свідчить відомий досвід, саме від реалізованого рівня легітимації і контролю виконання критичних процедур управління, зрештою, залежить фактичний рівень безпеки застосування відповідних систем та/або комплексів автоматизації. Ця ситуація однаковою мірою характерна, як при вирішенні завдань управління технічними засобами і технологічними процесами, так і під час реалізації систем, де об'єктами управління виступають безпосередньо люди [1-2].

В якості прикладів необхідності використання підсистем *(або засобів*) захисту від несанкціонованих дій (НСД) можна навести наступні:

– підтвердження процедур делегування *(тобто, тимчасової передачі)* повноважень управління заданим категоріям персоналу базових ІС, котрі задіяні при виконанні критичних циклів управління;

– санкціонування виконання особливо важливих процедур управління *(наприклад, підтвердження індикативних грошових транзакцій, дистанційне підтвердження виконання процедури знищення спеціальних баз даних тощо)*;

– зміна поточних режимів роботи контрольованих технічних засобів та/або критичних технологічних процесів (*наприклад, зміна поточного режиму роботи енергоагрегату)*;

– санкціонування доступу персоналу до «контрольованих» вантажів та критичних об'єктів техногенної інфраструктури *(віддалене спільне розблокування електронних пломб та елементів доступу до технічних об'єктів*);

– санкціонування доступу обслуговуючого персоналу до зміни діючих параметрів роботи елементів підсистеми захисту від НСД на об'єктах базової ІС *(у тому числі розблокування кодоблокуючих пристроїв підсистеми (або засобів) захисту від НСД);*
– централізоване «скидання» поточних блокувань кодоблокуючих пристроїв підсистеми захисту від НСД, які здійснені внаслідок фіксації спроб реалізації несанкціонованих дій (*наприклад, при підтвердженні фактів ненавмисного порушення порядку реалізації контрольованих процедур управління в межах передбачених циклів управління базової ІС*);
– централізоване блокування апаратури та/або доступу до даних на контрольованих ланках управління базової системи (*або окремих об'єктів базової ІС)* при спробах компрометації елементів підсистеми та/або засобів захисту від НСД;
– підтвердження процедури видачі разових повноважень персоналу нижніх ланок управління базової ІС, що мають тимчасові чи інші обмеження *(наприклад, з геолокації та/або кратності їх використання)*;
– санкціонування змін в діючій конфігурації структури системи управління базової ІС *(наприклад, активація режиму роботи через інстанцію або запуск гіпервізорів функціонального VR-розширення окремих елементів базової ІС*);
– спільне «скидання» параметрів *(програмованих уставок)* таймерів контролю виконання критичних процедур та ін.

Підтримка розглянутого вище функціоналу забезпечується шляхом комплексної інтеграції до складу базової ІС, відповідних елементів підсистеми захисту від НСД (*чи засобів санкціонування повноважень*). При цьому під «легітимацією процедур управління» слід розуміти процес надання необхідного рівня гарантій щодо безумовної відповідності реалізованих процедур управління вимогам технічної, експлуатаційної та нормативної документації.

Забезпечення зазначених гарантій виконується шляхом реалізації комплексу організаційно-технічних заходів, які передбачають глибоку взаємну інтеграцію процесів інформаційної взаємодії систем, що сполучаються [1-2].

2. Основна частина

Розглянемо найбільш характерні варіанти інтеграції елементів двох систем, які забезпечують різний рівень взаємної транспарентності і ієрархічних відносин між базовою ІС та підсистемою (та/або комплексом засобів) захисту від НСД.

На рис. 1 представлені найбільш характерні варіанти інтеграції елементів системи захисту від НСД до складу базової ІС. Із представлених схем слід, що підвищення вимог до рівня функціональних можливостей і ступеня автономності навіть найпростішої реалізації комплексу засобів захисту від НСД *(див. рис. 1(а))*, поетапно підвищує статус цих засобів на рівень окремої підсистеми у складі базової ІС (*рис. 1(б)) – 1(в)*), доводячи її можливості до рівня незалежної системи (рис. 1(г)), яка має абсолютний пріоритет, стосовно контролю заданого переліку функціональних завдань базової ІС.

У варіанті, наведеному на рис. 1(а), елементи (*або програмне забезпечення)* комплексу засобів захисту від НСД, є складовою частиною окремих підсистем у складі базової ІС. Такий варіант реалізації захисту є не більш, ніж продовженням частини функцій наявних підсистем ІС, у які вони інтегровані, та не передбачає будь-якого «зовнішнього» (*технологічного*) входу. Така реалізація захисту від НСД можлива на етапі модернізації спеціального про-

грамного забезпечення відповідних підсистем базової ІС, але її можливості обмежуються рівнем логічних блокувань, із усіма наслідками, що звідси випливають…

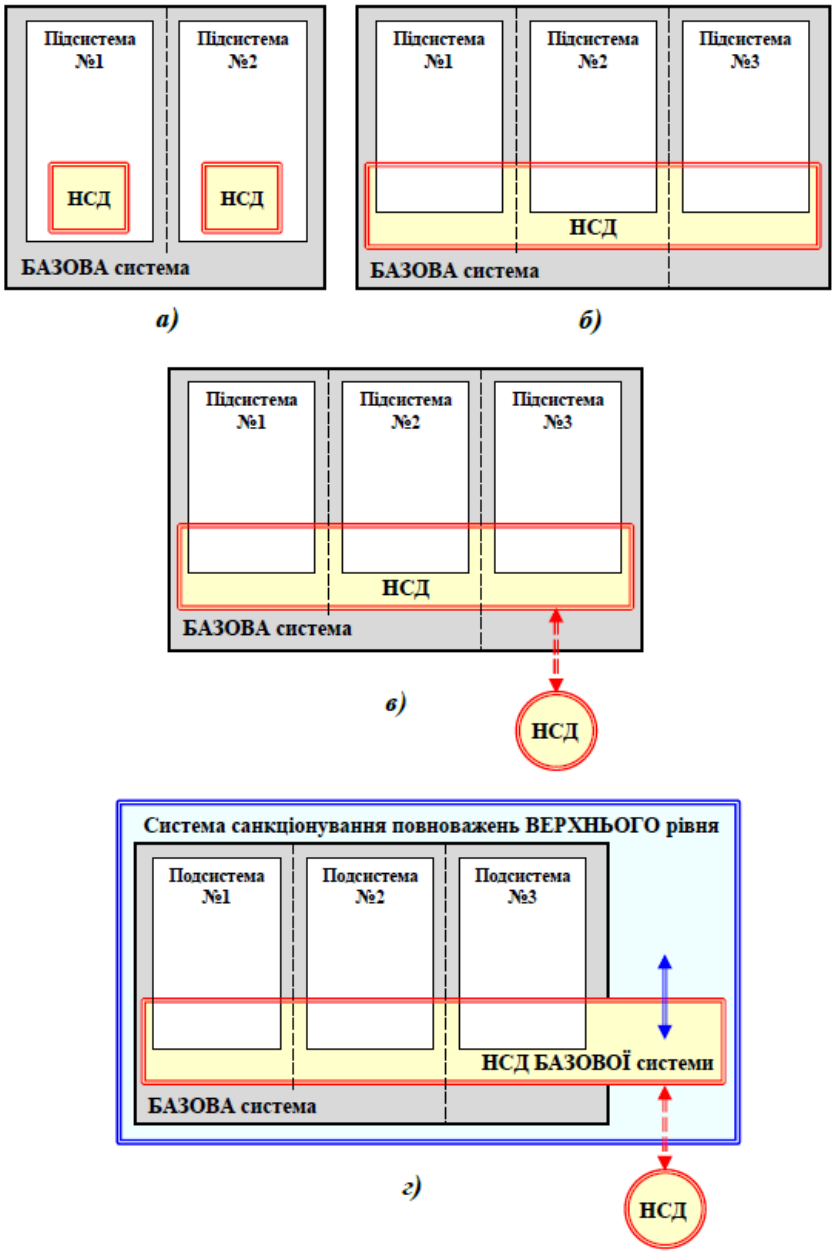

Рис. 1 – Варіанти інтеграції систем

Варіант взаємодії, представлений на рис.1(б) декілька розширює можливості комплексу засобів захисту від НСД до рівня однієї з підсистем в складі базової ІС. У цьому випадку логіка роботи складових елементів підсистеми захисту підпорядковується загальній логіці роботи базової ІС. Відповідно, перебуваючи на вищому ієрархічному рівні, базова ІС є провідною в частині регламентації складу функціональних завдань для підсистеми захисту від НСД, забезпечуючи можливість її діагностики та зміни параметрів налаштування. Принциповою відмінністю варіанта *1(б)* від *1(а)* є те, що в даному випадку засоби підсистеми захисту від НСД контролюють «точки» сполучення *(інтерфейси взаємодії*) складових підсистем базової ІС. За рахунок цього, підвищується загальний рівень безпеки та усувається можливість створення обхідних ланцюгів (*в т.ч. можливість імітації або програмної емуляції окремих елементів*) у найважливіших сегментах базової системи.

У даному випадку виконавчі елементи підсистеми захисту можуть вводити необхідні блокування *(або навпаки ініціювати запуск відповідних процесів, наприклад, знищення даних)* на рівні взаємодії окремих підсистем базової ІС, залежно від заданих для неї (підсистеми захисту) критеріїв оцінки поточного ступеня загроз, щодо реалізації НСД.

Такими параметрами можуть бути:

– перевищення заданої кількості спроб введення нелегітимних *(в т.ч. помилкових)* команд управління в межах здійсненні циклів управління базової ІС;

– порушення порядку спільних дій персоналом базової ІС під час реалізації особливо важливих *(критичних)* процедур управління;

– перевищення встановлених значень процедурних тайм-слотів, в т.ч. при реалізації *критичних* процедур управління базової ІС;

– порушення порядку доступу до елементів підсистеми захисту від НСД *(в т.ч. порушення цілісності інтерфейсів та/або порядку обміну інформацією між елементами підсистеми захисту, що розміщуються на різних рівнях (та/або підсистемах) базової ІС)* та ін.

Варіант інтеграції, що представлений на рис.1(в), знижує ступінь функціональної залежності підсистеми захисту від особливостей поточних режимів роботи і дій персоналу базової системи. У даному випадку система захисту структурно є підсистемою базової ІС, проте має незалежний від неї канал взаємодії *(входу в систему захисту)* із «зовнішніми» елементами цієї ж підсистеми. Залежно від особливостей реалізації базової ІС (*топологія, параметри розміщення інфраструктури, характеристики мобільності основних елементів та ін.*), у якості таких «зовнішніх» елементів може виступати автономна консоль обслуговування підсистеми захисту від НСД (*червоне коло, що позначено «НСД» на рис.1(в)*). Поява цього елемента в загальній структурі засобів управління «виводить» з функцій базової системи такі можливості, як:

– локальне управління параметрами роботи підсистеми захисту від НСД (*в межах діючих повноважень для обслуговуючого її персоналу*);

– робота з даними log-файлів підсистеми захисту *(тобто функції аудиту інцидентів)*;

– розблокування (*локально або спільно з персоналом даної ланки управління базової ІС*) кодоблокуючих пристроїв підсистеми захисту від НСД;

– можливість взаємодії з персоналом вищої ланки управління базової ІС, минаючи залучення персоналу цієї ланки (*об'єкта*) управління

– оновлення програмного забезпечення елементів підсистеми захисту та ін.

Таким чином, в даному випадку, базова система втрачає можливість адміністрування функцій для підсистеми захисту від НСД, зберігаючи лише логічну взаємодію спеціальних алгоритмів у циклах контролю виконання критичних процедур управління.

Зрештою, рис.1(*г*) відображає варіант інтеграції систем, при якому підсистема захисту від НСД фактично виведена за рамки функціональної залежності від базової ІС, а їх взаємодію слід розглядати, як завдання з поєднання двох практично незалежних систем. В даному випадку система захисту від НСД, що інтегрується з базовою ІС, може мати не тільки локальний канал взаємодії зі своїми «зовнішніми» елементами (рис.1(*в*)), але й бути частиною іншої, ієрархічно більш високорівневої системи, яка вирішує завдання загального контролю та легітимації циклів управління для цілої множини систем, що об'єднані спільними цілями та/або функціональними задачами.

У загальному випадку, розгляд тематики питань, що розглядаються, диктує необхідність проведення відповідного аналізу загроз, щодо забезпечуваного рівня легітимації про-

цедур формування і виконання найбільш важливих (критичних) команд управління. Існування подібних загроз багато в чому обумовлено виникненням відповідних передумов здійснення НСД, характерних для різних умов експлуатації та застосування за призначенням, як самої базової системи в цілому, так і окремих засобів автоматизації, що входять до її складу [3]. При цьому, визначення передумов здійснення НСД та подальший всебічний аналіз першопричин їх появи, слід проводити спираючись на результати широкої систематизації досвіду розробки і експлуатації відповідних ІС, та засобів захисту від НСД, з одного боку, і аналітичного прогнозу їх подальшого розвитку, з іншої сторони.

3. Висновки

1. При загальній схожості базових ідей та цільових установок, особливості проектування підсистем (засобів) захисту від НСД, у кожному конкретному випадку мають свою яскраво виражену специфіку та обмеження.

2. Декларований рівень легітимації основних процедур управління визначає необхідний рівень інтеграції аналізованих систем.

3. Рівень функціональної залежності підсистеми захисту від НСД від поточних режимів роботи базової системи та дій персоналу визначається переліком та змістом покладених на неї задач, а також ступенем автономізації основних функцій захисту.

4. Розміщення виконавчих елементів підсистеми захисту від НСД у місцях сполучення основних підсистем базової ІС, при одночасному підвищенні рівня автономізації її основних функцій, є найбільш правильною стратегією при проектуванні та створенні таких систем.

5. Оперативне розблокування виконавчих елементів підсистеми захисту від НСД, можливе шляхом реалізації спільних дій персоналу скомпрометованої системи та представників органів управління верхніх ланок управління базової ІС (*режим спільного розблокування*).

6. Актуальність розглянутої проблематики обумовлена впливом 5 основних факторів:
   – суттєвими змінами у змісті та формах реалізації процедур управління;
   – тенденцією до розосередження основних елементів систем, що захищаються;
   – підвищенням вимог до рівня компетентності персоналу;
   – високим ступенем технологічних ризиків сучасних техногенних комплексів (*енерговузли, транспортні системи, хімічні виробництва та ін.*) при збереженні значного рівня внутрішніх загроз (*інсайд, саботаж і т.п.*);
   – масштабністю та швидкоплинністю настання наслідків за успішної реалізації НСП, безвідносно їх субстантивного змісту.

Список літератури

[1] Сербин, В. & Малахов, С. Захист від несанкціонованих дій в сучасних інформаційних системах. Проблеми інформатизації: матеріали 7-ї міжнар. наук.-техн. конф., 13-15 листопада 2019 р. Харків, Україна. Вилучено з http://repository.kpi.kharkov.ua/handle/KhPI-Press/42752

[2] Сербин, В. & Малахов, С. Особливості інтеграції підсистем захисту від несанкціонованих дій в сучасних інформаційних системах і комплексах автоматизації. Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: матеріали 11-ї міжнар. наук.-техн. конф., 08-09 квітня 2021 р. Харків, Україна: ДП «Південний державний проектно-конструкторський та науково-дослідницький інститут авіаційної промисловості». Вилучено з http://repository.kpi.kharkov.ua/handle/KhPI-Press/52020

[3] Мелкозьорова, О., Лєсная, Ю., & Малахов, С. (2022). Особливості забезпечення захисту від НСД в сучасних інформаційних системах. InterConf, (97). Вилучено з https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/18428

Received: on June 2022. Accepted: on August 2022.

Authors:

Olha Melkozerova, Ph.D., Associate Professor Department of Security of Information Systems and Technologies, V.N. Karazin Kharkiv National University, Ukraine.

ORCID ID https://orcid.org/0000-0002-1134-2925
E-mail: olha.melkozerova@karazin.ua

Yuliia Liesnaia, student of the Department of Security of Information Systems and Technologies, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: xa12284109@student.karazin.ua

Serhii Malakhov, Ph.D., Senior Researcher, Computer Science Department, V.N. Karazin Kharkiv National University, Ukraine.
ORCID ID https://orcid.org/0000-0001-8826-1616
E-mail: mailgate@meta.ua

Peculiarities of the integration of systems of protection against unsanctioned actions in modern information systems.

Abstract. The purpose of this material is a brief review of the main options for integrating elements of systems (subsystems) of protection against unsanctioned activities (NSA) into information systems (IS) for various purposes. It is noted that the degree and method of mutual integration of the main systems are the result of the projection of the realized hierarchical relations between them. Attention is drawn to the fact that, depending on the operating conditions and the purpose of the base system, a significant reconfiguration of the logic of their relationship is possible, regarding the depth of mutual control and the possibilities of blocking the specified control functions (and/or critical processes). It is emphasized that with the general similarity of the basic ideas, the specific features of the design of protection subsystems against NSA in each case have their own specifics and limitations. Attention is focused on the fact that the declared level of legitimation of management procedures determines the required level of integration of interfaced systems (device). It is concluded that the level of functional dependence of the protection subsystem on the current modes of operation of the basic information system and the actions of its personnel is determined by the content of the (NSA) tasks assigned to it.

Keywords: information systems; delegation of authority; control link; joint actions; sanctioning; unsanctioned activities (NSA); information security.