УДК 004.056.53

к.т.н. Овсянніков В.В. (ВІТІ)
Паламарчук Н.А. (ВІТІ)
Паламарчук С.А. (ВІТІ)
Черниш Ю.О. (ВІТІ)

ПІДХОДИ ДО ФОРМУВАННЯ ВИМОГ З ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Одним із завдань при створенні захищених автоматизованих систем (АС) є визначення вимог до захисту інформації та формування функціонального профілю захищеності інформації в автоматизованій системі, який міститься в технічному завданні на створення комплексної системи захисту інформації в АС. Сучасний методологічний апарат дозволяє визначати, моделювати та оцінювати стан захищеності об'єктів захисту на експертному рівні, однак ключовим залишається саме процес формулювання вимог до захисту при взаємодії Замовників, Розробників та експертів, які оцінюють автоматизовану систему згідно етапів та стадій її створення (проектування, визначення вимог, розробки експлуатаційної документації, тощо). Формування вимог до захисту інформації проведено за рахунок зіставлення міжнародного стандарту ДСТУ ISO/IEC 15408 та нормативних документів системи технічного захисту інформації України та розглянуто на прикладі вимог до ідентифікації та автентифікації. Як варіант, в технічному завданні на створення комплексної системи захисту інформації в автоматизованій системі, пропонується формулювання вимог до захисту інформації проводити згідно термінології ДСТУ ISO/IEC 15408 (оперує термінологією ІТ-сфери), в доповнення до нормативних документів системи технічного захисту інформації. Це дозволить структурувати та деталізувати опис вимог до захисту інформації для Розробників автоматизованих систем щодо розробки списку атрибутів безпеки, правил початкової асоціації атрибутів безпеки користувачів, правил керування змінами атрибутів безпеки користувачів, списку поєднуваних механізмів автентифікації, тощо.

***Ключові слова**: автентифікація та ідентифікація користувачів, автоматизована система (інформаційно-телекомунікаційна система), атрибути доступу користувачів, електронні довірчі послуги, комплексна система захисту інформації (КСЗІ), розмежування доступу користувачів, технічний захист інформації (ТЗІ).*

Овсянников В.В., Паламарчук Н.А., Паламарчук С.А, Черныш Ю.О. Подходы к формированию требований идентификация и аутентификация в автоматизированных системах военного назначения.

Одной из задач при создании защищенных автоматизированных систем (АС) является определение требований к защите информации и формирования функционального профиля защищенности информации в автоматизированной системе, который содержится в техническом задании на создание комплексной системы защиты информации в АС. Современный методологический аппарат позволяет определять, моделировать и оценивать состояние защищенности объектов защиты на экспертном уровне, однако ключевым остается именно процесс формулирования требований к защите при взаимодействии Заказчиков, Разработчиков и экспертов, которые оценивают автоматизированную систему согласно этапов и стадий ее создания (проектирование, определение требований, разработки эксплуатационной документации и т.д.). Формирование требований к защите информации проведено за счет сопоставления международного стандарта ISO/IEC 15408 и нормативных документов системы технической защиты информации Украины и рассмотрено на примере требований к идентификации и аутентификации. Как вариант, в техническом задании на создание комплексной системы защиты информации в автоматизированной системе, предлагается формулирование требований к защите информации проводить согласно терминологии ISO/IEC 15408 (оперирует терминологией ИТ-сферы), в дополнение к нормативным документам системы технической защиты информации. Это позволит структурировать и детализировать описание требований к защите информации для Разработчиков автоматизированных систем по разработке списка атрибутов безопасности, правил начальной ассоциации атрибутов безопасности пользователей, правил управления изменениями атрибутов безопасности пользователей, списка объединяемых механизмов аутентификации и тому подобное.

***Ключевые слова:** аутентификация и идентификация пользователей, автоматизированная система (информационно-телекоммуникационная система), атрибуты доступа пользователей, электронные доверительные услуги, комплексная система защиты информации (КСЗИ), разграничение доступа пользователей, техническая защита информации (ТЗИ).*

***V. Ovsyannikov, N. Palamarchuk, S. Palamarchuk, Y. Cherhish Approaches to the formation of requirements with identification and authentication in automated military systems.** One of the tasks in creating protected automated systems (AS) is to determine the requirements for information security and the formation of a functional profile of information security in an automated system, which is contained in the terms of reference for the creation of an integrated information protection system in AS. The modern methodological apparatus allows us to determine, simulate and evaluate the state of protection of objects of protection at the expert level, however, the key is the process of formulating protection requirements in the interaction of Customers, Developers and experts who evaluate an automated system according to the stages and stages of its creation (design, determination of requirements,*

development of operational documentation, etc.). The requirements for information protection were formed by comparing the international standard ISO/IEC 15408 and the regulatory documents of the technical information protection system of Ukraine and examined by the example of identification and authentication requirements. Alternatively, in the terms of reference for the creation of an integrated information security system in an automated system, it is proposed that the information security requirements be formulated in accordance with ISO/IEC 15408 terminology (operates with IT terminology), in addition to the regulatory documents of the information security technical system. This will allow you to structure and detail the description of information security requirements specifically for Developers of automated systems for developing a list of security attributes, rules for the initial association of user security attributes, rules for managing changes to user security attributes, a list of federated authentication mechanisms, and the like.

Key words: *user authentication and identification, automated system (information and telecommunication system), user access attributes, electronic trust services, integrated information protection system (ISIS), user access delimitation, technical information protection (TI).*

Постановка завдання в загальному вигляді. Сучасні автоматизовані системи (АС) військового призначення відображають взаємодію структурних підрозділів Збройних Сил України (ЗСУ), є розподіленими та за класифікацією відносяться до автоматизованих систем класу 2 та класу 3. Інформаційна взаємодія таких АС організовується та здійснюється з урахуванням особливостей діяльності тих чи інших структурних підрозділів ЗСУ, тобто взаємодія службових осіб не лише в ієрархічній підпорядкованості підрозділів „по вертикалі", але і взаємодія суміжних підрозділів – „по горизонталі", тоді як керування доступом до інформації покладається на керівника структурного підрозділу/установи. Звідси, доступ посадових осіб до інформації в АС має бути організований таким чином, щоб забезпечити їх автентифікацію та унеможливити подвійне управління доступом.

Обробка інформації в системах, в яких циркулює інформація з обмеженим доступом або інформація, яка потребує захисту згідно законодавства, дозволяється лише з використанням захищеної технології. Технологія обробки інформації є захищеною, якщо вона містить організаційні заходи та програмно-технічні засоби захисту (комплекси засобів захисту від несанкціонованого доступу (КЗЗ від НСД), криптографічного захисту інформації, цифрового підпису, тощо), що забезпечують виконання вимог із захисту інформації та реалізовується створенням комплексної системи захисту інформації в АС. Загалом, доступ до інформації, яка захищається в АС, надається лише ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися. Підсистема ідентифікації та автентифікації є одним з ключових елементів системи захисту від несанкціонованого доступу будь-якої АС [1, 4, 6].

Вимоги із захисту інформації для кожної АС висуваються в технічному завданні на створення АС (окремим розділом) або деталізуються в окремому технічному завданні на створення комплексної системи захисту інформації (КСЗІ) в цій АС. Складністю при проектуванні та створенні захищених систем є деталізація опису вимог із захисту інформації та неоднозначне їх трактування замовниками та розробниками систем (розробники за звичай, працюють під визначену/засвоєну технологію програмування, яка не завжди надає гнучку можливість реалізації послуг безпеки та їх інтеграцію в систему, що створюється (або спеціальне програмне забезпечення), і як наслідок, призводить до формальної реалізації вимог нормативних документів системи ТЗІ. Одним із підходів до формування вимог із захисту інформації в АС, в доповнення до НД ТЗІ, може бути використання міжнародних стандартів із захисту інформації, а саме ДСТУ ISO/IEC 15408-2 „Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги" (гармонізовані Україною в 2017 році, але на практиці не використовуються), які відображають універсальний систематизований каталог функціональних вимог безпеки й передбачають можливість їх деталізації й розширення за певними правилами [5]. В практичній діяльності, вимоги із захисту інформації конкретизуються у функціях безпеки, які в подальшому реалізуються через множину механізмів та засобів безпеки конкретного об'єкту [12].

Відповідно, пропонується в технічному завданні на створення комплексної системи захисту інформації в автоматизованій системі, формулювання вимог до захисту інформації

проводити згідно термінології ДСТУ ISO/IEC 15408 (оперує термінологією ІТ-сфери. Це дозволить структурувати та деталізувати опис вимог до захисту інформації для Розробників автоматизованих систем.

Аналіз останніх публікацій. Зазвичай, основна увага українських науковців (Юдін О.К., Корченко О.О., Хорошко В.О., Бурячок В.Л. та ін.) приділяється стандартам для оцінки захищеності інформації, що має потужний теоретико-методологічний апарат та доволі часто використовується при експертному оцінюванні [11 – 13]. Практичне ж використання, НД ТЗІ 2.5-004-99 „Критерії оцінки захищеності інформації у комп'ютерних системах від НСД" та НД ТЗІ 2.5-005-99 „Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від НСД" упорядковано затвердженням НД ТЗІ 3.7-003-05 „Порядок проведення робіт із створення КСЗІ в ІТС".

В той же час, ряд експертів вважають НД ТЗІ 2.5-004-99 доволі застарілими, а виконання завдань на тих чи інших етапах створення КСЗІ досить формальними, які не в повній мірі дозволяють визначити адекватність висунутих вимог, не вдаючись детально в технології обробки інформації та в реалізацію відповідних засобів захисту [12, 13]. За рівнем систематизації, повноти та можливості деталізації вимог, універсальності, гнучкості в застосуванні для оцінки якості реалізації, найбільш вдалим із існуючих є міжнародний стандарт ISO/IEC 15408, зіставлення якого з НД ТЗІ 2.5-004-99 дозволить досягти більш якісного опису та деталізації при розробці вимог до захисту інформації.

Так, в НД ТЗІ 2.5-004-99 розглядаються вимоги до функцій захисту, які розбиті на чотири групи, кожна з яких описує вимоги, що забезпечують захист від загроз одного із чотирьох типів (конфіденційності, цілісності, доступності та спостереженості). ДСТУ ISO/IEC 15408 встановлює сукупність функціональних компонентів як стандартний спосіб вираження функціональних вимог до об'єкту. Містить каталог функціональних компонентів, сімейств і класів (11). Кожен клас містить декілька сімейств (1, 2, 3…), функціональні компоненти яких ранжуються в межах класу, можуть мати декілька рівнів (від 1 до 7).

Метою статті є розробка підходу до формування вимог із захисту інформації в автоматизованих системах за рахунок зіставлення нормативних документів системи технічного захисту інформації України (НД ТЗІ), а саме НД ТЗІ 2.5-004-99 та міжнародного стандарту ДСТУ ISO/IEC 15408, на прикладі вимог до ідентифікації та автентифікації (відповідних послуг безпеки).

Виклад основного матеріалу дослідження. Нормативно-правові документи, що регламентують формування вимог до захисту інформації в рамках діяльності організаційних структур (в тому числі, в ЗСУ) та обробки інформації в АС, в яких циркулює інформація, яка потребує захисту згідно законодавства, представлені на рис. 1. Формування вимог із захисту інформації в АС базується на основі забезпечення властивостей конфіденційності, цілісності та доступності інформації, а також спостереженості системи, які складають функціональний профіль захищеності інформації в АС (послуги безпеки відповідного рівня) [2 – 4].

Вимоги із захисту інформації від несанкціонованого доступу в АС класу 1 та класу 2 визначені відповідними НД ТЗІ. Для АС класу 3 нормативного документу не передбачено, вимоги розробляються в ході проектування системи, з врахуванням особливостей її функціонування та діяльності структурних підрозділів, які її експлуатують.

До особливостей діяльності може бути віднесено: функціонування структурних підрозділів на різних рівнях ієрархії (ланках управління); наявність обмеження доступу до інформації (в сукупності чи за окремими показниками); необхідність централізованого (розподіленого) зберігання інформації та розмежування доступу до неї та ін. Зазначене, є визначальним при формуванні вимог до захисту та аналізується для кожної АС окремо під час обстеження [8].

Враховуючи практичний досвід робіт зі створення КСЗІ для потреб ЗСУ та за результатами зіставлення НД ТЗІ з ДСТУ ISO/IEC (рис. 2) можливо визначити вимоги, які реалізуватимуть наступні послуги безпеки: ідентифікація та автентифікація, достовірний канал, автентифікація відправника та отримувача, ідентифікація і автентифікація при обміні.

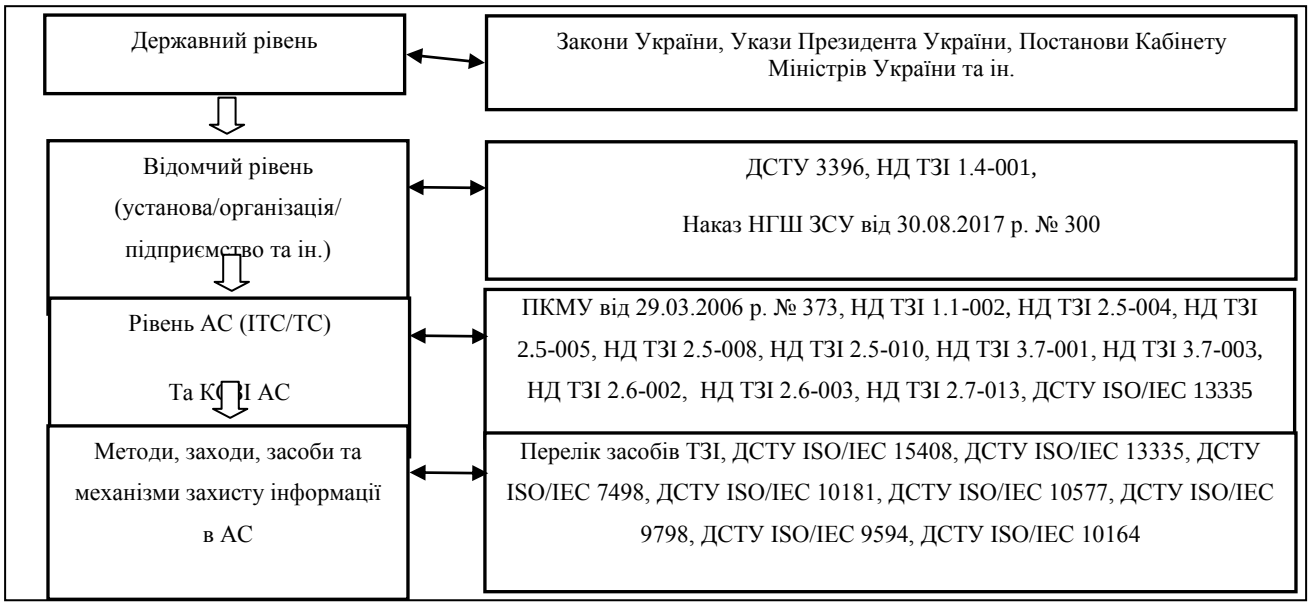

Рис. 1. Нормативно-правові документи, які регламентують формування вимог до захисту інформації

Рис. 2. Зіставлення НД ТЗІ з ДСТУ ISO/IEC

Згідно НД ТЗІ 2.5-004-99, послуга „**Ідентифікація та автентифікація"** дозволяє КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до АС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації (табл. 1). Розрізняють 3 рівні ідентифікації та автентифікації, які є досить умовними та формально відображають вимоги до складових процедури. Важливим є те, що ідентифікація

та автентифікація здійснюється за виконання необхідної умови – послуги достовірний канал (НК), яка гарантує те, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається).

Таблиця 1 – Рівні послуги „Ідентифікація та автентифікація”

НИ-1. Зовнішня ідентифікація і автентифікація	**НИ-2. Одиночна ідентифікація і автентифікація**	**НИ-3. Множинна ідентифікація і автентифікація**
1. Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ		
2. Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен		
з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача	автентифікувати цього користувача з використанням захищеного механізму	автентифікувати цього користувача з використанням захищених механізмів двох або більше типів
—	**3.** КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування	
НЕОБХІДНІ УМОВИ: НЕМАЄ	НЕОБХІДНІ УМОВИ: НК-1	

Як зазначалося, в міжнародному стандарті ДСТУ ISO/IEC 15408 функціональні вимоги описано більш деталізовано, з іншою структурою (рис. 3), розглянемо їх на прикладі послуг „Ідентифікація та автентифікація” та „Достовірний канал”.

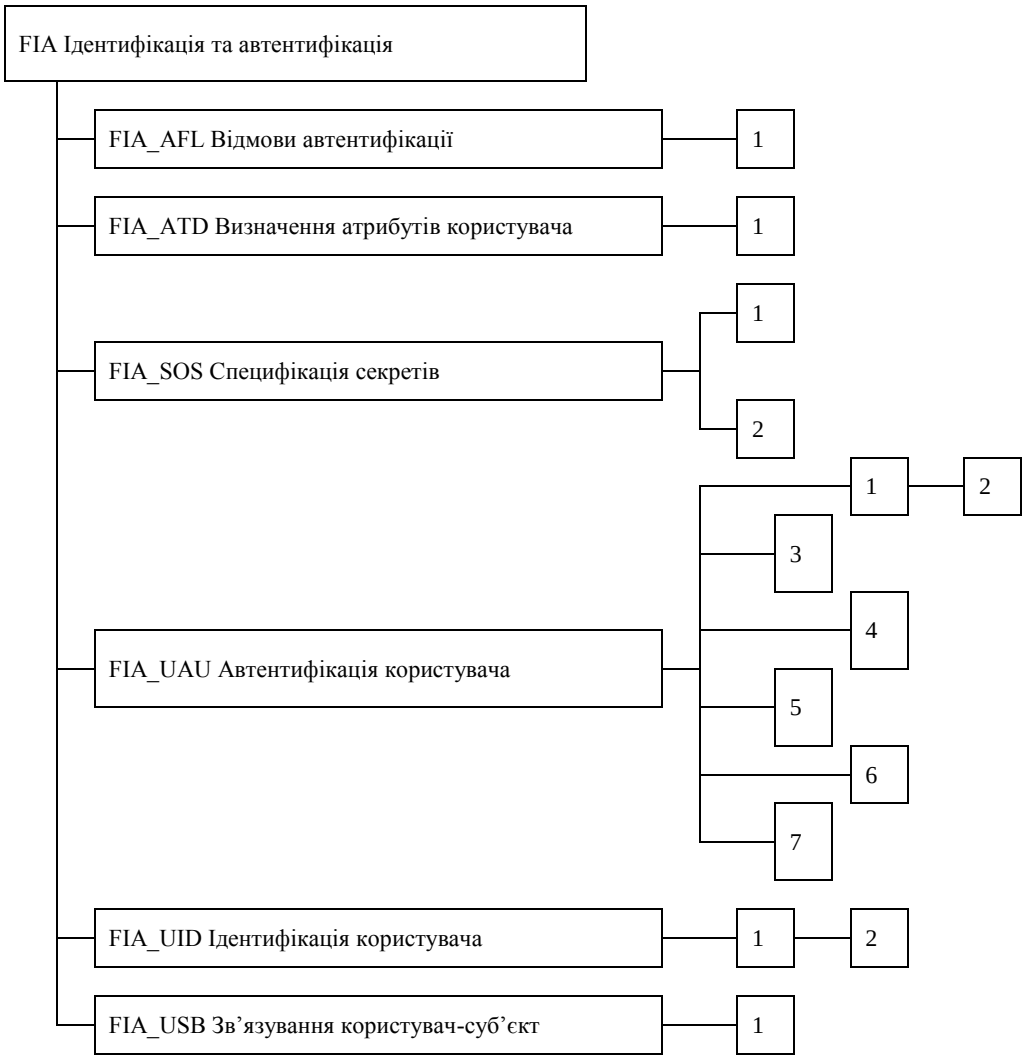

Рис. 3. Декомпозиція класу „Ідентифікація та автентифікація”

Сімейства класу FIA „**Ідентифікація та автентифікація”** визначають вимоги до функцій, що встановлює і верифікує заявлений ідентифікатор кожного користувача. Ідентифікація та автентифікація потрібні для забезпечення асоціації користувачів з відповідними атрибутами безпеки (такими, як ідентифікатор, групи, ролі, рівні безпеки або цілісності). Послуги ідентифікаційних систем розглядаються за наступними декомпозиціями:

Сімейство FIA_UID „**Ідентифікація користувача”** призначено для визначення ідентифікатора користувача (FIA_UID.1 „Вибір моменту часу ідентифікації”, FIA_UID.2 „Ідентифікація до будь-яких дій користувача”), визначає умови, при яких від користувачів потрібна власна ідентифікація до виконання при посередництві КЗЗ будь-яких інших дій, що вимагають ідентифікації користувача.

Сімейство FIA_UAU „**Автентифікація користувача”** призначено для верифікації ідентифікатора користувача (FIA_UAU.1 „Вибір моменту часу автентифікації”, FIA_UAU.2 „Автентифікація до будь-яких дій користувача”, FIA_UAU.3 „Автентифікація, захищена від підробок”, FIA_UAU.4 „Механізми одноразової автентифікації”, FIA_UAU.5 „Поєднання механізмів автентифікації”, FIA_UAU.6 „Повторна автентифікація” та FIA_UAU.7 „Автентифікація з захищеним зворотним зв’язком”), визначає типи механізмів автентифікації користувача, що надаються КЗЗ та ті атрибути, на яких необхідно базувати механізми автентифікації користувача.

Сімейство FIA_AFL „**Відмови автентифікації”** призначене для визначення обмеженого числа повторних невдалих спроб автентифікації. FIA_AFL.1 „Обробка відмов автентифікації” містить вимогу, щоб КЗЗ були здатні перервати процес відкриття сеансу після певного числа неуспішних спроб автентифікації. Параметрами, що визначають можливе число спроб автентифікації, також можуть бути кількість спроб, інтервал часу.

Сімейство FIA_ATD „**Визначення атрибутів користувача”** призначене для визначення атрибутів користувачів, що застосовуються при здійсненні політики безпеки. Всі уповноважені користувачі можуть, крім ідентифікатора користувача, мати інші атрибути безпеки, що застосовуються при здійсненні політики безпеки. Визначає вимоги для асоціації атрибутів безпеки з користувачами відповідно до необхідності підтримки політики безпеки, дозволяє підтримувати атрибути безпеки для кожного користувача індивідуально.

Сімейство FIA_USB „**Зв’язування користувач-суб’єкт”** призначене для коректної асоціації атрибутів безпеки кожного вповноваженого користувача. Для роботи з об’єктом автентифікований користувач активізує будь-який суб’єкт. Атрибути безпеки користувача асоціюються з цим суб'єктом. Визначає вимоги зі створення та супроводження асоціації атрибутів безпеки користувача з суб'єктом, що діє від імені користувача.

Сімейство FIA_SOS „**Специфікація секретів”** призначене для генерації і верифікації секретів, які задовольняють встановленої метрики. Визначає вимоги до механізмів, які реалізують певну метрику якості для наданих секретів і генерують секрети, що задовольняють певній метриці.

Таблиця 2 – Рівні послуги „Достовірний канал”

НК-1. Однонаправлений достовірний канал	**НК-2. Двонаправлений достовірний канал**
Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ	
Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем	Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації та у випадках, коли необхідний прямий зв'язок користувач/КЗЗ або КЗЗ/користувач. Зв'язок з використанням даного каналу повинен ініціюватися користувачем або КЗЗ
—	Обмін з використанням достовірного каналу, що ініціює КЗЗ, повинен бути однозначно ідентифікований як такий і має відбутися тільки після позитивного підтвердження готовності до обміну з боку користувача
НЕОБХІДНІ УМОВИ: НЕМАЄ	

Згідно НД ТЗІ 2.5-004-99, послуга „**Достовірний канал”** гарантує те, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається). Рівні послуги

ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін (табл. 2).

Згідно ДСТУ ISO/IEC 15408, послузі „Достовірний канал” відповідає клас FTP: Довірений маршрут/канал (рис. 4).

Сімейства цього класу (FTP_ITC Довірений канал передачі між КЗЗ та FTP_TRP Довірений маршрут) надають вимоги як до довіреного маршруту зв’язку між користувачами і КЗЗ, так і до довіреного каналу зв'язку між КЗЗ й іншими довіреними продуктами ІТ.

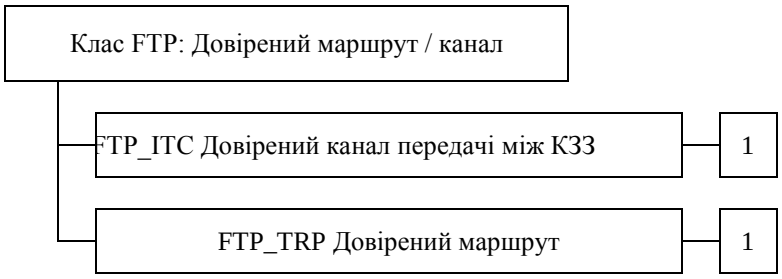

Рис. 4. Декомпозиція класу „Довірений маршрут/канал”

Таким чином з’ясовано, що набір послуги „**Ідентифікація та автентифікація”** (Зовнішня ідентифікація і автентифікації НИ-1, Одиночна ідентифікація і автентифікації НИ-2 та Множинна ідентифікація і автентифікація НИ-3), а також „**Достовірний канал”** (Однонаправлений достовірний канал НК-1 та двонаправлений достовірний канал НК-2) мають відповідні класи в ДСТУ ISO/IEC 15408, однак містять інші класи сімейств послуг та їх ранжирування, які більш деталізовано дозволять формувати вимоги до захисту інформації в АС. Так, послуга „Ідентифікація та автентифікація” згідно ДСТУ ISO/IEC 15408 (окрім зазначених вище) містить „FIA_AFL „Відмови автентифікації”, „FIA_ATD „Визначення атрибутів користувача”, „FIA_UAU „Автентифікація користувача”, „FIA_UID „Ідентифікація користувача” та “FIA_USB „Зв’язування користувач-суб’єкт”.

Наприклад, якщо в системі висувається вимога НИ-3. Множинна ідентифікація і автентифікація (див. табл.1), за результатами зіставлення отримуємо набір таких послуг:

для опису вимог рядка 1: „FIA_ATD 1.1. „Визначення атрибутів користувача”, „FIA_USB 1.1. „Зв’язування користувач-суб’єкт”.

для опису вимог рядка 2: „FIA_UID 2.1. „Ідентифікація до будь-яких дій користувача”, „FIA_UAU 2.1. „Автентифікація до будь-яких дій користувача” та „FIA_UAU 5.1. „Співвідношення механізмів автентифікації”.

Якщо в ТЗ на створення КСЗІ в АС визначені вимоги згідно ДСТУ ISO/IEC 15408, а не НД ТЗІ, то розробник системи вимушений для КЗЗ розробити список атрибутів безпеки; правила початкової асоціації атрибутів безпеки користувачів; правила керування змінами атрибутів безпеки користувачів; вимоги, щоб кожен користувач був успішно ідентифікований та автентифікований до дозволу будь-якої дії в системі; список поєднуваних механізмів автентифікації; правила, що описують, як поєднання механізмів автентифікації забезпечує автентифікацію.

Для послуг безпеки „Автентифікація відправника”, „Автентифікація отримувача” та „Ідентифікація і автентифікація при обміні” відсутня безпосередня відповідність вимог в НД ТЗІ 2.5-004-99 та ДСТУ ISO/IEC 15408. Дані послуги зіставляються згідно з НД ТЗІ 2.6-002-2015 „Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99” [7].

Згідно НД ТЗІ 2.5-004-99, послуга „**Автентифікація відправника”** дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем.

Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною (табл. 3).

Таблиця 3 – Рівні послуги „Автентифікація відправника”

НА-1: Базова автентифікація відправника	**НА-2: Автентифікація відправника з підтвердженням**
Політика автентифікації відправника, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем	
—	Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися для однозначного підтвердження належності об'єкта незалежною третьою стороною
Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації	
—	Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження належності об'єкта незалежною третьою стороною
НЕОБХІДНІ УМОВИ: НИ-1	

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація послуги НИ-1 (Зовнішня ідентифікація і автентифікація).

Згідно НД ТЗІ 2.6-002-2015, послуга зіставляється з наступними послугами (табл. 4).

Таблиця 4 – Зіставлення послуги „Автентифікація відправника”

НД ТЗІ 2.5-004-99	**ДСТУ ISO/IEC 15408-2-2001**
Автентифікація відправника (НА)	FCO_NRO Невідмовність відправлення. FCS_COP Криптографічні операції. FCS_CKM Управління криптографічними ключами.
	Необхідні умови (залежності)
	FIA_UID.1 Вибір моменту часу ідентифікації (клас Ідентифікація та автентифікація) FDP_ITC.1 Імпорт даних користувача без атрибутів безпеки (клас Захист даних користувача) FDP_ACC.1 Обмежене управління доступом або FDP_IFC.1 Обмежене управління інформаційними потоками (клас Захист даних користувача) FMT_MSA.2 Безпечні значення атрибутів безпеки (клас Управління безпекою) FMT_MSA.3 Ініціалізація статичних атрибутів (клас Управління безпекою)

Сімейство „FCO_NRO Невідмовність відправлення” (FCO_NRO.1 “Вибірковий доказ відправлення” та FCO_NRO.2 „Примусовий доказ відправлення”) забезпечує, що відправник інформації не зможе заперечувати факт відправлення інформації (рис. 5). Містить вимогу, щоб КЗЗ надали метод забезпечення того, що суб'єкту, який отримує інформацію під час обміну даними, надається свідоцтво відправлення інформації. Це свідоцтво може бути потім верифіковане цим суб'єктом або іншими суб'єктами.

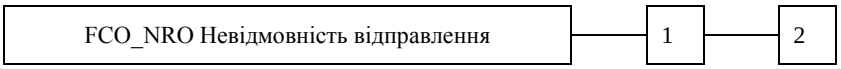

Рис. 5 Невідмовність відправлення

Сімейства „FCS_COP Криптографічні операції” та **„FCS_CKM Управління криптографічними ключами”** відносяться до класу криптографічної підтримки (рис. 6).

Криптографічними ключами необхідно керувати протягом усього їх життєвого циклу. **Сімейство FCS_CKM** визначає вимоги до наступних дій: FCS_CKM.1 „Генерація криптографічних ключів”, FCS_CKM.2 „Розподіл криптографічних ключів”, FCS_CKM.3 „Доступ до криптографічних ключів” та FCS_CKM.4 „Знищення криптографічних ключів”.

Необхідною умовою для виконання FCS_CKM Управління криптографічними ключами є виконання FMT_MSA.2 Безпечні значення атрибутів безпеки.

Сімейство FCS_COP Криптографічні операції. FCS_COP.1 „Криптографічні операції” містить вимоги, щоб криптографічні операції виконувалися відповідно до визначених

алгоритмів і з застосуванням криптографічних ключів певної довжини. Задані алгоритми і довжина криптографічних ключів можуть ґрунтуватися на прийнятому стандарті.

Рис. 6 Криптографічна підтримка

До типових криптографічних операцій належать: зашифрування і / або розшифрування даних, генерація і / або верифікація цифрових підписів, генерація криптографічних контрольних сум для забезпечення цілісності та / або верифікації контрольних сум, гешування (обчислення геш-образу повідомлення), зашифрування і / або розшифрування криптографічних ключів, узгодження криптографічних ключів.

Таким чином, послуга „**Автентифікація відправника”** (Базова автентифікація відправника НА-1, Автентифікація відправника з підтвердженням НА-2) не має відповідних послуг згідно ДСТУ ISO/IEC 15408, а зіставляється (комбінується) послугами FCO_NRO Невідмовність відправлення, FCS_COP Криптографічні операції, FCS_CKM Управління криптографічними ключами.

Необхідними умовами є FIA_UID.1 Вибір моменту часу ідентифікації, FDP_ITC.1 Імпорт даних користувача без атрибутів безпеки, FDP_ACC.1 Обмежене управління доступом або FDP_IFC.1 Обмежене управління інформаційними потоками, FMT_MSA.2 Безпечні значення атрибутів безпеки та FMT_MSA.3 Ініціалізація статичних атрибутів). Згідно НД ТЗІ 2.5-004-99, послуга „**Автентифікація отримувача”** дає можливість забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною (табл. 5).

Таблиця 5 – Рівні послуги „Автентифікація отримувача”

НП-1: Базова автентифікація отримувача	**НП-2: Автентифікація отримувача з підтвердженням**
Політика автентифікації одержувача, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-одержувача і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був одержаний певним користувачем	
—	Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися незалежною третьою стороною для однозначного підтвердження факту одержання об'єкта
Встановлення одержувача має виконуватися на підставі затвердженого протоколу автентифікації	
—	Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження незалежною третьою стороною факту одержання об'єкта
НЕОБХІДНІ УМОВИ: НИ-1	

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація послуги НИ-1 (Зовнішня ідентифікація і автентифікація).

Згідно НД ТЗІ 2.6-002-2015 послуга зіставляється з наступними послугами (табл. 6).

Таблиця 6 – Зіставлення послуги „Автентифікація отримувача”

НД ТЗІ 2.5-004-99	**ДСТУ ISO/IEC 15408-2-2001**
Автентифікація отримувача (НП)	FCO_NRR Невідмовність отримання. FCS_COP Криптографічні операції. FCS_CKM Управління криптографічними ключами.
	Необхідні умови (залежності) ті ж, що і в табл. 4

Таким чином, послуга „**Автентифікація отримувача”** (Базова автентифікація отримувача НП-1 та Автентифікація отримувача з підтвердженням НП-2) комбінується послугами FCO_NRR Невідмовність отримання, FCS_COP Криптографічні операції, FCS_CKM Управління криптографічними ключами.

Згідно НД ТЗІ 2.5-004-99, послуга „**Ідентифікація і автентифікація при обміні”** дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації (табл. 7).

Таблиця 7 – Рівні послуги „Ідентифікація і автентифікація при обміні”

НВ-1: Автентифікація вузла	**НВ-2: Автентифікація джерела даних**	**НВ-3: Автентифікація з підтвердженням**
Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації		
—	КЗЗ повинен використовувати захищені механізми для встановлення джерела кожного об'єкта, що експортується та імпортується	
—		Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження джерела об'єкта незалежною третьою стороною

Згідно НД ТЗІ 2.6-002-2015 послуга зіставляється з наступними послугами (табл. 8).

Таблиця 8 – Зіставлення послуги „Ідентифікація і автентифікація при обміні”

НД ТЗІ 2.5-004-99	**ДСТУ ISO/IEC 15408-2-2001**
Ідентифікація і автентифікація при обміні (НР)	FTP_ITC Довірений канал передачі між КЗЗ. FCS_COP Криптографічні операції. FCS_CKM Управління криптографічними ключами. FDP_DAU.1 Базова автентифікація даних (клас Захист даних користувача)
	Необхідні умови (залежності) ті ж, що і в табл. 4

FTP_ITC Довірений канал передачі між КЗЗ.

FDP_DAU.1 Базова автентифікація даних (клас Захист даних користувача) містить вимогу, щоб КЗЗ були здатні до надання гарантії справжності інформації, що міститься в об’єктах (*наприклад,* документах).

Таким чином, послуга „**Ідентифікація і автентифікація при обміні”** (Автентифікація вузла НВ-1, Автентифікація джерела даних НВ-2 та Автентифікація з підтвердженням НВ-3) комбінується послугами FTP_ITC Довірений канал передачі між КЗЗ, FCS_COP Криптографічні операції, FCS_CKM Управління криптографічними ключами, FDP_DAU.1 Базова автентифікація даних.

Висновки. Проаналізовано можливості розширення вимог НД ТЗІ 2.5-004-99 набором послуг безпеки, які визначені ДСТУ ISO/IEC 15408 та забезпечують виконання автентичності, цілісності інформації та ідентифікації службових осіб. Запропонований підхід надає можливості Замовнику більш детально формувати вимоги до захисту інформації в конкретній АС, із включенням їх до функціонального профілю захищеності інформації, який міститься в технічному завданні на створення АС (КСЗІ в АС) та відповідно, вибирати Розробника системи, який буде спроможний їх реалізувати в повному обсязі. З врахуванням зазначеного, доцільна розробка відомчих нормативних документів ЗСУ для їх використання Замовниками та Розробниками при проектуванні АС та створенні КСЗІ в них.

Подальші дослідження доцільно спрямувати на розробку методик оцінки захищеності захищеності інформації в АС з врахуванням запропонованого підходу.

ЛІТЕРАТУРА

1. Постанова Кабінету Міністрів України № 373 від 29.03.2006 р. „Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах” (зі змінами).

2. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

3. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації у комп’ютерних системах від несанкціонованого доступу.

4. НД ТЗІ 2.5-008-02 Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу „2” (зі змінами).

5. ДСТУ ISO/IEC 15408-2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги.

6. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі (зі змінами).

7. НД ТЗІ 2.6-002-2015 Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99.

8. Овсянніков В.В., Мальцева І.Р., Паламарчук Н.А., Паламарчук С.А. Проблемні питання захисту інформаційних ресурсів в ІТС органів публічної влади // IX НПС „Пріоритетні напрямки розвитку ТКС та мереж спеціального призначення” з урахуванням досвіду АТО, 25.11.2016 р.: Доповіді та тези доповідей. К.: ВІТІ, 2016. – с.137.

9. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов / П.Н. Девянин, О.О. Михальский, Д.И. Правиков и др.- М.: Радио и связь, 2000. – 192 с.

10. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.

11. Гладун А.Я., Хала К.О. Таксономія стандартів інформаційної безпеки // Інформаційні технології: наука, технології, інновації. 2017, № 2. – с. 53 – 64.

12. Косенко И.В., Усачёва О.А., Стадниченко М.Г. Формализация требований гарантий безопасности (в соответствии со стандартом ISO / IEC 15408) на основе CASE-подхода.// Кібернетика та системний аналіз. Збірник наукових праць Харківського університету Повітряних Сил, 2016, випуск 1(46) – с. 93 – 98.

13. Бурячок В.Л., Козачок В.А., Бурячок Л.В., Складанний П.М. Пентестінг як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах / Сучасний захист інформації №3, К.: 2015 – с. 4 – 12.