УДК 004.056.53

Процюк Ю.О. (ВІТІ)
Паламарчук Н.А. (ВІТІ)
Паламарчук С.А. (ВІТІ)
Штонда Р.М. (ВІТІ)

ПРОПОЗИЦІЇ З ВИБОРУ ОРГАНІЗАЦІЙНО-ТЕХНІЧНИХ РІШЕНЬ ДЛЯ АВТОМАТИЗОВАНИХ СИСТЕМ З ВРАХУВАННЯМ ВИМОГ ДО ЇХ ЗАХИСТУ

Захист інформації в автоматизованих системах є складовою частиною робіт з їх створення та експлуатації, і повинен здійснюватися на всіх етапах життєвого циклу АС. Діюча нормативно-правова база України щодо проектування та створення автоматизованих систем (АС) та комплексних систем захисту інформації (КСЗІ) *в них, дозволяє одночасно створювати АС та КСЗІ. Однак, доволі часто роботи зі створення АС виконуються окремо від створення КСЗІ, без узгодження організаційно-технічних рішень, що в подальшому призводить до потреби їх змін через неможливість реалізувати вимоги із захисту інформації. Крім цього, досить часто виконання функціональних задач доцільно реалізувати на тій чи іншій архітектурі АС та/або за допомогою окремого спеціалізованого програмного забезпеченням (до спеціалізованого програмного забезпеченням також висуваються вимоги, в тому числі і до захисту інформації). В разі необхідності, деталізація вимог можлива на рівні окремо розробленого технічного завдання на створення спеціалізованого програмного забезпечення.*

На основі нормативних документів визначено фактори, які впливають на вибір організаційно-технічних рішень для створення захищених АС, серед яких класифікація інформації, що обробляється, клас та архітектура АС, вид управління доступу та місце зберігання інформації, тощо. Запропоновано варіант організаційно-технічних рішень для створення захищеної АС з врахуванням особливостей діяльності Збройних Сил України, на прикладі реалізації підсистеми несанкціонованого доступу в АС.

Ключові слова*: автоматизована система (інформаційно-телекомунікаційна система), атрибути доступу користувачів, комплексна система захисту інформації, розмежування доступу користувачів, автентифікація.*

Процюк Ю.А., Паламарчук Н.А., Паламарчук С.А, Штонда Р.М. Предложения по выбору организационно-технических решений для автоматизированных систем с учетом требований по их защите. *Защита информации в автоматизированных системах (АС) является составной частью работ по их созданию и эксплуатации, и должна осуществляться на всех этапах жизненного цикла АС. Действующая нормативно-правовая база Украины по проектированию и созданию автоматизированных систем и комплексных систем защиты информации (КСЗИ) в них, позволяет одновременно создавать АС и КСЗИ. Однако, довольно часто работы по созданию АС выполняются отдельно от создания КСЗИ, без согласования организационно-технических решений, что в дальнейшем приводит к необходимости их изменения из-за невозможности реализовать требования по защите информации. Кроме этого, достаточно часто выполнение функциональных задач целесообразно реализовать на той или иной архитектуре АС и/или с помощью отдельного специализированного программного обеспечения (к специализированному программному обеспечению также выдвигаются требования, в том числе и к защите информации). В случае необходимости, детализация требований возможна на уровне отдельно разработанного технического задания на создание специализированного программного обеспечения.*

На основе нормативных документов определены факторы, влияющие на выбор организационно-технических решений для создания защищенных АС, среди которых классификация обрабатываемой информации, класс и архитектура АС, вид управления доступа и место хранения информации, и тому подобное. Предложен вариант организационно-технических решений для создания защищенной АС с учетом особенностей деятельности Вооруженных Сил Украины, на примере реализации подсистемы несанкционированного доступа в АС.

Ключевые слова: *автоматизированная система (информационно-телекоммуникационная система), атрибуты доступа пользователей, комплексная система защиты информации, разграничение доступа пользователей, аутентификация.*

Y.* Protsiuk, *N. Palamarchuk, S. Palamarchuk, R. Shtonda Proposals for the selection of organizational and technical solutions for automated systems, taking into account the requirements for their protection. *Information protection in automated systems (AS) is an integral part of the work on their creation and operation, and should be carried out at all stages of the life cycle of AS. The current regulatory framework of Ukraine for the design and creation of automated systems and integrated information protection systems (ISIS) in them, allows you to simultaneously create AS and ISIS. However, quite often, the work of the AS creation is carried out separately from the creation of ISIS, without the coordination of organizational and technical solutions, which further leads to the need to change them due to the inability to implement the requirements for information protection. In addition, quite often it is advisable to implement functional tasks on one or another AS architecture and / or using separate specialized software*

(requirements for specialized software are also put forward, including information protection). If necessary, detailed requirements are possible at the level of a separately developed technical task for the creation of specialized software.

On the basis of regulatory documents, factors were determined that affect the choice of organizational and technical solutions for creating ASs secure, including classification of the processed information, AS class and architecture, type of access control and information storage location, etc. A variant of organizational and technical solutions is proposed for creating a secure nuclear power plant, taking into account the specifics of the activities of the Armed Forces of Ukraine on the example of the implementation of the unauthorized access subsystem in the nuclear power plant.

Key words: *automated system (information and telecommunication system), user access attributes, integrated information protection system, user access control, authentication.*

Постановка завдання в загальному вигляді. Активне використання автоматизованих систем (АС) для розв'язання широкого спектру практичних завдань, в тому числі і в Збройних Силах України, вимагає підвищеної уваги розробників до їх захисту. Централізація управління віддзеркалює наявність тих чи інших підрозділів (відділів, служб, управлінь) на відповідних рівнях – тактичному, оперативному, стратегічному, а автоматизація діяльності, окрім технічної реалізації, має визначати організаційний порядок обробки інформації (в т.ч. і інформації з обмеженим доступом) в кожній конкретній автоматизованій системі, що зазвичай, зв’язує всю вертикаль органів військового управління (ОВУ).

Також, слід акцентувати увагу на те, що враховуючи територіальний розподіл ОВУ, а відповідно і автоматизовані системи, що створюються, відноситимуться до автоматизованих систем класу 3 (АС кл. 3), для складових частин (модулів) яких може бути визначена різна політика безпеки. Велика кількість інформації, часто потребує структуризації та реалізовується побудовою різноманітних баз даних. Не рідко, Замовником приймається рішення спочатку створити АС, для обробки відкритої інформації, а з часом розширити систему для обробки інформації з обмеженим доступом. З самого початку, це шлях до невиправданих фінансових, часових та інтелектуальних витрат, який не дасть бажаного результату. Оскільки, згідно вимог законодавства, реалізація певних вимог із захисту інформації в АС (особливо вимога конфіденційності) повинна забезпечуватися визначеними засобами, відповідно, АС створюється/модернізується заново з усіма наслідками, які випливають [8].

Окрім того, якщо в АС планується обробка інформації з різними грифами обмеження доступу, передбачається велика кількість користувачів, які матимуть різні повноваженнями на обробку інформації (запис, читання, видалення тощо) тоді ускладнюється питання щодо надання доступу цим користувачам, тобто налаштування комплексу засобів захисту від несанкціонованого доступу коли стандартних атрибутів доступу (ім’я користувача в системі та пароль) вже недостатньо.

Одним із підходів у вирішенні цього питання може бути вибір архітектури побудови АС та визначення додаткових атрибутів доступу користувача на етапі проектування КСЗІ.

Аналіз останніх публікацій. Питанням проектування та створення захищених АС, в тому числі спеціального призначення, на вітчизняному рівні приділяється надзвичайна увага такими вченими як Конахович Г.Ф., Юдін О.К., Дудикевич В.Б., Корченко О.Г. Моделювання таких систем має здійснюватись комплексно. В публікаціях Дудикевича В.Б., Юдіна О.К., розглядаються моделі систем за складовими інформаційних даних, загроз та механізмів захисту. Частково, Костяк М. Ю. розглядає особливості проектування захищених інформаційних мереж спеціального призначення, їх архітектуру та управління процесом обміну інформацією [9 – 10]. С.Г. Семенов, досліджує технології розмежування доступу для захисту даних в комп'ютерній системі [11]. Теоретичні підходи до систем, що реально проектуються та створюються потребують взаємозв’язку та узгодженості в питаннях реалізації організаційно-технічних рішень та подальшого оцінювання їх захищеності.

Метою статті є розробка пропозицій з вибору організаційно-технічних рішень для створення автоматизованих систем з врахуванням вимог до їх захисту на основі практичного досвіду створення АС та КСЗІ в них.

Виклад основного матеріалу. Поняття автоматизованих систем визначено в державному стандарті [1], автоматизована система – це організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності, людей та персоналу, що здійснює цю діяльність.

Згідно [3], автоматизована система – це організаційно-технічна система, що реалізує інформаційну технологію і об'єднує обчислювальну систему, фізичне середовище, персонал і інформацію, яка обробляється. Інформація, яка належить до державних інформаційних ресурсів або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в АС із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. КСЗІ в системі повинна складатись з організаційних заходів та апаратно-програмних засобів захисту інформації (комплексу засобів захисту від несанкціонованого доступу, засобів криптографічного захисту інформації, засобів електронного підпису тощо).

Відповідно, об'єктами захисту в системі є інформація, що обробляється та програмне забезпечення, яке призначено для обробки інформації. АС в цілому, і її окремі підсистеми, повинні будуватись одночасно зі створенням КСЗІ, як на систему так і на її підсистеми.

Захищені автоматизовані системи не розглядаються окремо від інформації, яка в них обробляється та обов'язково враховується вплив навколишнього середовища функціонування. Засоби захисту інформації реалізовані в обчислювальній системі, розглядаються як підсистема захисту від НСД у складі КСЗІ (є предметом розгляду даної статті). Захист від фізичного НСД до компонентів обчислювальної системи в статті не розглядається, однак однозначно повинне бути розуміння, що фізичний захист та обмеження доступу організаційними заходами передує реалізації технічної захищеності. Очевидно, що характеристики фізичного середовища, персоналу, оброблюваної інформації та організаційної підсистеми істотно будуть впливати на вимоги до функцій захисту, що реалізуються обчислювальною системою [3].

Загалом, порядок створення КСЗІ в АС, вимоги до етапів робіт, документації, тощо визначені в [5] та низці інших керівних документів. Беручи до уваги вимоги нормативних документів [2 – 6], можливо виділити ряд факторів, які впливатимуть на вибір організаційно-технічних рішень для створення захищених АС (табл. 1).

Таблиця 1

Фактори, які впливають на вибір рішень для створення захищених АС

№	Найменування фактору	Коротка характеристика	Примітки
1	Наявність грифу обмеження доступу до інформації, що оброблятиметься в АС. Класифікація інформації	Інформація з обмеженим доступом, що становить державну таємницю (таємно, цілком таємно тощо)	Вимоги із захисту інформації від НСД (вимога К, Ц, Д) та від витоку технічними каналами
		Службова інформація	Вимоги із захисту інформації від НСД (вимога К, Ц, Д)
		Конфіденційна інформація	
		Відкрита інформація, вимога щодо захисту якої встановлена законом	Вимоги щодо захисту інформації від НСД (вимога Ц, Д)
2	Клас АС	Клас "1" – одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності	Вимоги із захисту інформації формуються з врахуванням грифу обмеження доступу до інформації та/або необхідності передачі інформації через незахищене середовище
		Клас "2" – локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності	
		Клас "3" – розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності	
3	Вид управління доступу до інформації в АС	Довірче керуванням доступом – засоби захисту дозволяють звичайним користувачам управляти (довіряють керування) потоками інформації між	Однакові повноваження користувачів

		іншими користувачами і об'єктами свого домену (наприклад, на підставі права володіння об'єктами)	
		Адміністративне керуванням доступом – засоби захисту дозволяють управляти потоками інформації між користувачами і об'єктами тільки спеціально авторизованим користувачам	Наявність адміністраторів
4	Інтегрованість АС	Неінтегрована. Вирішуються однотипні задачі	Єдині вимоги до захисту інформації в АС
		Інтегрована. Складові елементи ІТС (модулі) будуються за типовими організаційно-технічними рішеннями, які вирішують різнотипні задачі	Різні вимоги до політики безпеки інформації, до функціонального профілю захищеності інформації кожного з модулів в АС
5	Архітектура АС	АРМ поєднані в локальну мережу (без виділеного сервера)	Інформація зберігається на АРМ, ЛОМ – для передачі інформації між ними. Лише для груп користувачів з однаковими повноваженнями
		АРМ поєднані в локальну мережу (з виділеним сервером)	Доступ користувачів до всіх ресурсів ЛОМ
		Клієнт-серверна архітектура	Інформація структурується у види визначеної БД, яка розміщується на окремому сервері. Дозволяє організувати роботу багатьох користувачів з різними повноваженнями АРМ користувачів є клієнтами даного сервера
		Трьохрівнева архітектура	До сервера БД має доступ додатковий сервер – сервер додатків. Клієнти взаємодіють лише з сервером додатків і не мають доступу до сервера БД. Дозволяє організувати гнучке налаштування системи розмежування доступу
		Технологія розподілених обчислень	Наявність багатьох серверів, на кожному з яких функціонує визначена служба, що виконує визначений сервіс. Збереження даних забезпечується використанням кількох фізично розділених примірників баз даних, об’єднаних у логічний кластер. Для взаємодії з клієнтами також встановлюються сервери додатків. Дозволяє забезпечувати глобальний доступ всім користувачам до всієї інформації. Складна з точки зору захисту інформації
6	Місце зберігання інформації	На АРМ користувача (розподілене зберігання)	Різні технології обробки інформації та організаційний порядок надання доступу до інформації
		На сервері (база даних, централізоване зберігання)	
		На зовнішньому носії інформації (різноманітні накопичувачі інформації)	

Однак, не дивлячись на наявність зазначених документів, вимоги для захисту інформації в АС різного функціонального призначення не так однозначні. Більшість АС, в тій чи іншій мірі, використовують бази даних (БД). Захищеність інформації з обмеженим доступом у всій АС, практично повністю визначається захищеністю БД.

В АС класу 1 використовують реляційні БД (частіше всього MS Access). В цих випадках, забезпечення цілісності та конфіденційності інформації, не потребує особливих зусиль. Колективна робота з інформацією, навіть в невеликих об'ємах (*наприклад*, в локальній мережі – АС класу 2), суттєво ускладнює захист БД. В першу чергу, з'являється загроза для конфіденційності та цілісності при передачі інформації. По-друге, при організації колективної роботи виникають дві загрози, які відсутні в АС класу 1, це навмисне порушення встановлених правил розмежування доступу зловмисником, що знаходиться в цій мережі та одночасна спроба двох користувачів внести зміни в БД (джерелом загрози цілісності є необхідність легальним користувачам вносити зміни незалежно один від одного). Усунути цю загрозу можливо за рахунок правильної організації блокування спільного доступу, яке планується розробником АС, та як правило, не потребує додаткових заходів при розробці КСЗІ. В АС класу 3 (територіально-розподілених системах), забезпечення цілісності та конфіденційності ще більше ускладнюється через збільшення масштабів мережі, в межах якої може знаходитись зловмисник. Для обміну інформацією в таких системах використовуються відкриті мережі та системи зв'язку (включаючи мережу Інтернет). Також, в АС класу 3 військового призначення стає важливою специфічна особливість інформації, а саме, вимоги до конфіденційності інформації пов'язані не лише зі змістом, а й з обсягом інформації однотипного змісту, тобто, у військовій сфері узагальнення даних за відповідну ланку управління може призвести до підвищення грифу обмеження доступу. *Наприклад,* згідно ЗВДТ п. 1.1.4 – відомості про організацію або здійснення взаємодії військ (сил) у цілому щодо: бригади, полку, окремого батальйону (до них прирівняних) … – „Таємно"; виду, спеціальних військ, оперативного командування, повітряного командування, тактичної групи (до них прирівняних) ЗС… – „Цілком таємно". Також, в деяких випадках, гриф обмеження доступу не повністю характеризує вимоги до захисту інформації, і для інформації одного типу вимоги можуть відрізнятися. *Наприклад*, в АС циркулює відкрита інформація, однаковий доступ на ознайомлення з якою мають всі користувачі (інформація загальнодоступна для всіх користувачів), однак створювати цю інформацію та вносити зміни до неї можуть лише користувачі з відповідними повноваженнями (можливо навіть в залежності від територіальної приналежності).

Враховуючи, що АС класу 3 є своєрідною великою системою доцільно надавати доступ не кожному користувачеві окремо, а об'єднувати їх у своєрідні категорії/групи користувачів з певними ролями (за функціональною діяльністю), які в свою чергу мають право на виконання певних сценаріїв в АС. Правила розмежування доступу передбачають зіставлення інформації за визначеними класифікаційними ознаками з відповідними групами користувачів, які окрім основних атрибутів доступу, можуть мати додаткові (розробляються для конкретної АС). В загальному, до основних атрибутів доступу відносяться ім'я користувача в системі та пароль. Додатковими атрибутами для АС класу 3 можливо визначити територіальну приналежність, вид інформації, тип (група) користувача та ін.

Визначення додаткових атрибутів, врахування факторів, зазначених в табл. 1. та особливостей функціонування АС (структурного підрозділу ЗС України) надасть можливість здійснювати більш гнучке налаштування прав доступу користувачів.

Так, *наприклад* користувачі системи, які мають право на створення, редагування та читання інформації в межах повноважень, можна виділити у так звану групу користувачів типу 1, користувачів які мають право тільки ознайомлюватись з відповідною інформацією в межах повноважень – у групу користувачів типу 2, окремо виділяємо адміністраторів (системний, безпеки, баз даних тощо), які обслуговуватимуть АС та матимуть доступ лише до технологічної інформації.

З врахуванням зазначеного, пропонується варіант побудови захищеної АС кл. 3 на основі клієнт-серверної архітектури, основні елементи системи багаторівневого захисту

наведені на рис. 1, основні завдання щодо розмежування доступу користувачів можливо реалізувати на рівні спеціалізованого програмного забезпечення АС. У випадку клієнт-серверної архітектури вся інформація структурується у види визначеної БД, яка розміщується на окремому сервері. Всі задачі, виконуються на сервері, на АРМ інформація не зберігається, не обробляється, лише відображається, АРМ посадових осіб в АС є клієнтами даного сервера. На сервері розміщується система керування базою даних (СКБД), яка забезпечує пошук інформації за запитом клієнтів та її обробку, в залежності від функціонального призначення АС. Розмежування доступу користувачів до інформації здійснюється через додатковий сервер – сервер додатків (трьохрівнева архітектура). Клієнти взаємодіють лише з сервером додатків і не мають безпосереднього доступу до сервера БД.

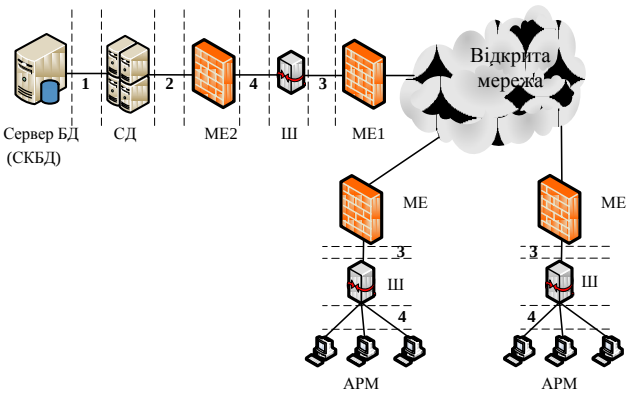

Рис. 1 Основні елементи системи багаторівневого захисту АС

Де СКБД – система керування БД, в якій зберігається вся інформація за АС;

СД – сервер додатків, забезпечує автентифікацію користувачів та надає дані з БД відповідно до правил розмежування доступ, повинен мати два мережевих адаптери, з метою запобігання доступу до СКБД в обхід нього;

МЕ 1 – мережевий екран, блокує атаки з відкритої мережі;

МЕ 2 – мережевий екран, блокує атаки зловмисників, які знаходяться в мережі АС;

1, 2, 3 – підмережі 1, 2, 3, входять до декількох різних зон захисту, в залежності від призначення АС, в цих зонах можуть розміщуватися додаткові елементи АС;

4 – мережа АС;

Ш – шифратор, що забезпечує шифрування всієї інформації, яка передається через відкриту мережу (канал зв'язку).

Більшість елементів системи прозорі для інформації, яку отримують користувачі згідно правил розмежування доступу. Для цих користувачів логічна структура АС є простою і зрозумілою (рис. 2). Різні спроби отримати доступ до даних, які зберігаються в БД, з порушенням встановлених правил розмежування доступу в АС, блокуються елементами зон захисту 1, 2, 3 відповідно. З точки зору захисту інформації, 3-рівнева архітектура є найкращою, оскільки на сервері додатків, крім реалізації складної бізнес-логіки, можливо організувати гнучке налаштування системи розмежування доступу до інформації, коли існує велика кількість користувачів, які одночасно працюють з одним і тим же набором даних, з різними повноваженнями (W – запис, R – читання, …). При правильній організації, на АРМ клієнта відсутня можливість ввести в АС будь-які технічні засоби, програмне забезпечення або зберігати інформацію на зовнішні носії (за необхідності, можливо одразу виводити на друк). Крім того, в АС, в яких обробляється інформація з обмеженим доступом повинна бути реалізована множинна ідентифікація та автентифікація (послуга НИ-3) тобто з використанням захищених механізмів, *наприклад,* захищеного засобу електронного підпису.

Послуга реалізується шляхом ідентифікації користувачів згідно введеного логіну та автентифікації за встановленим протоколом на основі представленого захищеного засобу з даними автентифікації та паролю. Дані автентифікації захищаються від НСД, модифікації

або руйнування з використанням тих же механізмів, що і при реалізації послуг базова адміністративна конфіденційність та базова адміністративна цілісність (послуг КА-2, ЦА-2).

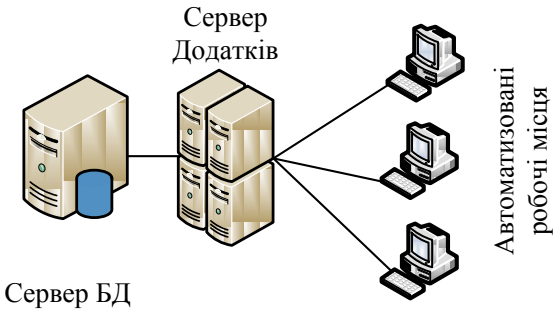

Рис. 2 Логічна структура АС

Такий підхід доцільний при створенні різноманітних реєстрів в т.ч. в ЗСУ (*наприклад*, облік ресурсів – особового складу, засобів озброєння та військової техніки, тощо). ***Висновки.*** В роботі розглянуто фактори, які впливають на вибір організаційно-технічних рішень для створення захищених АС. Для ЗС України запропоновано варіант створення захищеної АС, з використанням багаторівневої системи захисту, де ключову роль відіграє сервер додатків, через який реалізовано розмежування доступу.

Подальші дослідження доцільно направити на розробку підсистеми захисту від НСД в інтегрованій АС (яка створена на основі технології розподілених обчислень), співставлення вимог із захисту інформації та кіберзахисту з врахуванням національної та міжнародної нормативно-правової бази, а також стрімкого розвитку ІТ-сфери.

ЛІТЕРАТУРА

1. ДСТУ 2226-93 „Автоматизовані системи. Терміни та визначення”.

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

3. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.

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

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

6. Овсянніков В.В., Паламарчук С.А., Черниш Ю.О., Шемендюк О.В. Підходи щодо захисту баз даних в ІТС спеціального призначення // VIII НПК „Пріоритетні напрямки розвитку ТКС та мереж спеціального призначення з урахуванням досвіду АТО”, 29.10.2015 р.: Доповіді та тези доповідей. К.: ВІТІ, 2015. – с. 140 – 141.

7. Дехтяр С.В., Маковецький О.М., Паламарчук Н.А., Процюк Ю.О. Організаційно-правові та практичні аспекти щодо впровадження електронного документообігу, систем обміну інформацією в органах державної влади України // VIII НПК „Пріоритетні напрямки розвитку ТКС та мереж спеціального призначення з урахуванням досвіду АТО”, 29.10.2015 р.: Доповіді та тези доповідей. К.: ВІТІ, 2015. – с. 91.

8. Овсянніков В.В., Паламарчук Н.А., Паламарчук С.А., Процюк Ю.О. Особливості створення захищених інформаційно-телекомунікаційних систем військового призначення. // X НПК “Пріоритетні напрямки розвитку телекомунікаційних. систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв’язку та автоматизації в АТО”, 9-10.11.17 р.: Доповіді та тези доповідей. К.: ВІТІ, 2017. – с. 178 – 179.

9. Костяк М.Ю., Пархуць Л.Т. Особливості проектування захищених інформаційних мереж спеціального призначення. Львів: НУЛП, 2016. – с. 88 – 92.

10. Конахович Г.Ф. Захист інформації в мережах передачі даних / Г.Ф. Конахович, О.Г. Корченко, О.К. Юдін. – К.: Видавництво ТОВ „НВП „ІНТЕРСЕРВІС”, 2009. – 716 с.

11. Семенов С.Г., Зміївська В.М., Голубенко А.В. Порівняльні дослідження технологій розмежування доступу для захисту даних в комп'ютерній системі // Системи обробки інформації. 2015, № 3 – с. 99 – 102.