Центральний науково-дослідний інститут
Збройних Сил України
Military Science. Vol. 1 No. 1. 2023

Аналіз протоколів передавання даних у перспективній автоматизованій системі обміну науковою (науково-технічною) інформацією у Збройних Силах України

Олексій Ноздрачов
заступник начальника інституту з морально-психологічного забезпечення
Центральний науково-дослідний інститут Збройних Сил України
03049, 28Б, просп. Повітрофлотський, Київ, Україна
e-mail: o.o.nozdrachov @post.mil.gov.ua

Микола Васянович
кандидат військових наук, старший дослідник
начальник центру
Центральний науково-дослідний інститут Збройних Сил України
03049, 28Б, просп. Повітрофлотський, Київ, Україна
e-mail: m.o.vasianovych@post.mil.gov.ua
ORCID: 0000-0002-8409-4774

Андрій Шнукало
старший науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, 28Б, просп. Повітрофлотський, Київ, Україна
e-mail: a.d.shnukalo@post.mil.gov.ua
ORCID: 0000-0002-1205-9953

Анотація. Актуальність дослідження обумовлена потребою визначення ефективних протоколів передавання даних, які забезпечують високу якість обслуговування і захищеність автоматизованих систем обміну інформацією у Збройних Силах України та їх складових.

У зв'язку з цим дана стаття спрямована на розкриття протоколів транспортного рівня мережних моделей TCP/IP та OSI – User Datagram Protocol, User Datagram Protocol Lite, Transmission Control Protocol, Multipath Transmission Control Protocol, Stream Control Transmission Protocol, Datagram Congestion Control Protocol, Reliable User Datagram Protocol з точки зору перспективи їх використання в автоматизованих системах обміну науковою (науково-технічною) інформацією у Збройних Силах України.

Провідними підходами для дослідження цієї проблеми є використання методів інформаційно-логічного аналізу, що дозволяють комплексно розглянути мережні моделі за допомогою порівняння.

Розглянуто близько 15 характеристик, зокрема: надійність передавання, контроль перенавантаження, багатопоточність. Ураховуючи вимоги та особливості перспективної автоматизованої системи обміну науковою (науково-технічною) інформацією у Збройних Силах України, було запропоновано використання певних технологічних комбінацій з протоколами вищого рівня для досягнення оптимального захисту даних. У результаті аналізу встановлено, що, відповідно до функцій автоматизованої системи обміну науковою (науково-технічною) інформацією, більш доцільно використовувати протокол Stream Control Transmission Protocol.

Матеріали статті становлять теоретичну цінність для проведення подальших наукових досліджень стосовно порушеної проблеми, а також практичну – для удосконалення військових інформаційних систем, відповідно до стандартів Північноатлантичного альянсу та викликів сьогодення у кіберпросторі.

Ключові слова: обмін даними, інформаційні технології, мережні технології, військово-наукові автоматизовані системи.

Вступ (Introduction)

Автоматизовані системи обміну науково-технічною інформацією у Збройних Силах України (ЗС України) мають важливе значення для забезпечення національної безпеки та оборони. Проте їхній розвиток та функціонування потребують застосування відповідних протоколів передавання даних, які забезпечують безпеку інформаційного обміну та надійність передавання даних без втрат у швидкості.

Однією із проблем, яка потребує уваги у цій сфері, є відсутність стандартів та єдиної системи протоколів передавання даних у системах обміну науково-технічною інформацією у ЗС України. Це призводить до труднощів у взаємодії різних систем, що може знижувати швидкість передавання даних, збільшувати ризики витоку інформації та порушувати конфіденційність даних.

Крім того, є проблема відповідності існуючих протоколів передавання даних сучасним вимогам до захисту інформації, зокрема до захисту від кібератак та кібершпигунства. Через недостатню безпеку та ефективність таких протоколів можуть виникнути значні загрози національній безпеці та обороні, тому їхній аналіз із можливістю подальшого вдосконалення та оптимізації є актуальним науково-практичним завданням.

Методологічна основа (Methodological Framework)

Автоматизовані системи обміну науковою (науково-технічною) інформацією (АСОНТІ) є спеціалізованими інформаційними системами, які використовуються для обміну науковими даними, статтями, дослідженнями, технічними відомостями тощо між науковими установами, ученими, дослідниками та іншими зацікавленими сторонами.

Ці системи забезпечують ефективний обмін науковою інформацією шляхом створення централізованого репозиторію, де можна зберігати, шукати та отримувати доступ до наукових публікацій і даних. Деякі АСОНТІ також надають можливість взаємодії між користувачами, наприклад, на форумах для обговорення досліджень або можливість коментувати статті.

Основні функції автоматизованих систем обміну науковою інформацією:

- зберігання та пошук інформації;
- класифікація та оброблення інформації;
- публікація та рецензування наукових матеріалів;
- взаємодія та співпраця;
- моніторинг інформації;
- оцінювання наукової продуктивності.

Розглядаючи перспективну автоматизовану систему обміну науковою (науково-технічною) інформацією у ЗС України та її головну специфіку – застосування у військовому середовищі, необхідно виділити ще низку основних необхідних функцій:

- конфіденційність та безпека;
- інтеграція з іншими військовими системами.

Виходячи з останніх двох функцій, можна стверджувати, що протоколи передавання даних у перспективній автоматизованій системі обміну науковою (науково-технічною) інформацією у ЗС України мають відповідати таким вимогам:

– надійність;
– захищеність;
– стандартизація;
– багатопоточність;
– контроль потоків даних;
– стійкість до відмов;
– підтримка використовуваних у ЗС України операційних систем.

Результати (Results)

Розглянемо протоколи транспортного рівня (табл. 1). У комп'ютерних мережах транспортний рівень є концептуальним поділом методів у багаторівневій архітектурі протоколів моделей TCP/IP (Transmission Control Protocol/Internet Protocol) та OSI (The Open Systems Interconnection model). Протоколи цього рівня надають послуги наскрізного зв'язку для додатків (Papastergiou, 2017).

User Datagram Protocol (UDP) (укр. Протокол датаграм користувача) – один із протоколів у стеку TCP/IP. Від протоколу TCP він відрізняється тим, що працює без встановлення з'єднання. UDP – один із найпростіших протоколів транспортного рівня моделі OSI, котрий виконує обмін повідомленнями (датаграмами) без підтвердження та гарантії доставки. При використанні протоколу UDP відповідальність за оброблення помилок і повторне передавання даних покладена на протокол рівнем вище. Але попри всі недоліки, протокол UDP є ефективним для серверів, що надсилають невеликі відповіді великій кількості клієнтів.

UDP Lite (полегшений UDP) – протокол без встановлення з'єднань, що належить до транспортного рівня моделі OSI і схожий на UDP. На відміну від UDP, у якому пакет або цілком захищений контрольною сумою або пакет цілком не захищений, UDP Lite допускає можливість часткових контрольних сум, які покривають лише частину датаграми, і таким чином можлива доставка частково пошкоджених пакетів. Це було створено для мультимедійних протоколів, у яких прийняти пакети із частково пошкодженим корисним навантаженням вважається більш доцільним варіантом, ніж не отримати пакет узагалі.

Transmission Control Protocol (TCP) (укр. Протокол керування передаванням) разом із протоколом IP є стрижневим протоколом Інтернету, який дав назву моделі TCP/IP. Протокол призначений для керування передаванням даних у комп'ютерних мережах, працює на транспортному рівні моделі OSI.

На відміну від іншого поширеного протоколу транспортного рівня UDP, TCP забезпечує надійну доставку даних від хоста-відправника до хоста-отримувача, для цього встановлюється логічний зв'язок між хостами. Таким чином, TCP належить до класу протоколів зі встановленим з'єднанням.

TCP отримує потоки даних від протоколів верхніх рівнів OSI-моделі, початковим джерелом яких є протоколи прикладного рівня, такі як HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP) та інші. Кожний протокол верхнього рівня має свій визначений TCP-порт.

TCP розбиває конкретний потік даних на порції та додає до кожної з них заголовок з номером послідовності. Отримані таким чином порції даних традиційно називаються TCP-сегментами. Далі кожний сегмент інкапсулюється в IP-пакет і передається через IP-протокол до хоста-отримувача.

Таблиця 1. Порівняння протоколів транспортного рівня

Характеристика	Протоколи						
	UDP	UDP-Lite	TCP	Multipath TCP	SCTP	DCCP	RUDP
Розмір заголовка пакета	8 байт	8 байт	20–60 байт	50–90 байт	12 байтів	12 або 16 байт	14+ байт
Типові витрати пакетів даних	8 байт	8 байт	20 байт	? байтів	44–48+ байт	12 або 16 байт	14 байт
Об'єкт пакета транспорт. рівня	Датаграма	Датаграма	Сегмент	Сегмент	Датаграма	Датаграма	Датаграма
Орієнтований на підключення	Ні	Ні	Так	Так	Так	Так	Так
Надійне транспортування	Ні	Ні	Так	Так	Так	Ні	Так
Зберігання меж повідомлення	Так	Так	Ні	Ні	Так	Так	Так
Доставка	Невпорядкована	Невпорядкована	Впорядкована	Впорядкована	Впорядкована / Невпорядкована	Невпорядкована	Невпорядкована
Контрольна сума	Так / Ні	Так	Так	Так	Так	Так	Так / Ні
Розмір контрольної суми	16 біт	16 біт	16 біт	16 біт	32 біти	16 біт	16 біт
Часткова контрольна сума	Ні	Так	Ні	Ні	Ні	Так	Ні
Блок максимального передавання шляху	Ні	Ні	Так	Так	Так	Так	?
Управління потоком	Ні	Ні	Так	Так	Так	Ні	Так
Контроль перевантаженості	Ні	Ні	Так	Так	Так	Так	?
Явне сповіщення про перевантаж.	Ні	Ні	Так	Так	Так	Так	?
Багатопоточність	Ні	Ні	Ні	Ні	Так	Ні	Ні
Multihoming	Ні	Ні	Ні	Так	Так	Ні	Ні
Розшарування / Алгоритм Нейгла	Ні	Ні	Так	Так	Так	Ні	?

Джерело: розроблено авторами на основі відкритих джерел даних.

Після надходження IP-пакета до хоста-отримувача перевіряють коректність отриманих даних у TCP-сегменті методом перерахування контрольної суми та переконуються у тому, що попередні сегменти даних також були успішно отримані. Після цього хост-отримувач надсилає запит до хоста-відправника про нове або повторне передавання порції даних, що

одночасно є підтвердженням того, що всі сегменти з номерами послідовності, меншими ніж номер нового запиту, були успішно отримані.

У свою чергу, TCP-сегменти деінкапсулюються з IP-пакетів, розміщуються в правильному порядку і з них вилучаються TCP-заголовки. Отриманий таким чином потік даних передається до того протоколу верхнього рівня, з якого первісно надійшли дані на стороні хоста-відправника.

Multipath TCP (MPTCP) (багатошляховий TCP) – це робота робочої групи Multipath TCP Інженерної групи Інтернету (IETF), яка спрямована на те, щоб дозволити з'єднанню протоколу керування передаванням (TCP) використовувати кілька шляхів для максимізації пропускної здатності та збільшення резервування.

У січні 2013 року IETF опублікувала специфікацію Multipath як експериментальний стандарт у RFC 6824. У березні 2020 року її замінили на специфікацію Multipath TCP v1 у RFC 8684.

Надлишковість, яку пропонує Multipath TCP, забезпечує інверсне мультиплексування ресурсів і таким чином збільшує пропускну здатність TCP до суми всіх доступних каналів на рівні зв'язку, замість використання одного, як вимагає стандартний TCP. MPTCP зворотно сумісний зі стандартним TCP.

Stream Control Transmission Protocol (SCTP) (укр. Протокол передавання з керуванням потоку) – протокол транспортного рівня в комп'ютерних мережах, створений у 2000 році в IETF. RFC 3286 містить технічний вступ до нього.

Як і будь-який інший протокол передавання даних транспортного рівня, SCTP працює аналогічно TCP або UDP. TCP і UDP працюють настільки по-різному, що проводити аналогію до них обох некоректно. Уся аналогія полягає в тому, що SCTP, TCP і UDP належать до одного і того самого рівня моделі OSI. Але насправді SCTP має в арсеналі широкий спектр нововведень, таких як багатопоточність, захист від SYN-flood, а також синхронне з'єднання між двома хостами на двох і більше незалежних фізичних каналах (multi-homing).

Datagram Congestion Control Protocol (DCCP) (укр. Протокол контролю перевантаження датаграм) – мережний протокол транспортного рівня, розроблений IETF. Прийнятий як стандарт у березні 2006 року, він надає механізми для відстеження перевантажень у мережі, уникаючи можливості використання механізмів прикладного рівня. Цей протокол не гарантує доставку інформації в потрібному порядку.

DCCP дуже ефективний для додатків, у яких дані, що прийшли не вчасно, стають непотрібними. Наприклад: потокове медіа-мовлення, онлайн-ігри і інтернет-телефонія. Головна особливість цих додатків полягає в тому, що старі повідомлення дуже швидко стають непотрібними, тому краще отримати нове повідомлення, ніж намагатися переслати старе. Але на цей момент більшість таких додатків самостійно реалізують відстеження перевантажень, а як протоколи передавання використовуються TCP або UDP.

Reliable Data Protocol (RDP) (укр. Надійний протокол даних) розроблений для забезпечення надійного передавання даних між пакетно-орієнтованими додатками. Спочатку він був розроблений для програм, що реалізують віддалене завантаження даних і усунення несправностей, проте його можна використовувати і в інших програмах, що вимагають надійного передавання повідомлень. Є дві версії RDP, описані у специфікаціях RFC 908 та RFC 1151 відповідно.

Reliable User Datagram Protocol (RUDP) (укр. Надійний протокол дейтаграм користувача) заснований на протоколі RDP для передавання телефонних сигналів через IP-мережі. Цей протокол не стандартизований, не має офіційної специфікації.

Протоколи RDP і RUDP використовуються у тих випадках, коли не можна застосовувати UDP через його ненадійність, а використання TCP спричиняє надто високу складність процесу передавання даних.

З точки зору надійності, такими, що забезпечують надійне транспортування, можна вважати протоколи: TCP, Multipath TCP, SCTP, RUDP.

Організація надійного транспортування у цих протоколах має деякі спільні особливості, але також відрізняється залежно від конкретного протоколу (Kurose, 2017).

TCP:

– використовує механізм підтвердження ACK (Acknowledgment), де отримувач повертає квитанцію (підтвердження) про успішне отримання кожного пакета;

– забезпечує виявлення й відновлення втрачених пакетів шляхом повторного передавання втрачених пакетів;

– використовує механізми контролю потоку, такі як вікно передавання (Window), для регулювання швидкості передавання даних відправника до отримувача.

Multipath TCP (MPTCP):

– розподіляє трафік між різними шляхами, використовуючи механізми керування потоком й розподілу навантаження;

– має механізми для виявлення й управління втратою пакетів, які враховують розподілений характер мережі з кількома шляхами;

– забезпечує можливість динамічного переключання між шляхами у разі зміни умов мережі.

SCTP:

– використовує механізми асоціацій (Association), каналів і потоків для організації передавання даних;

– має механізми для виявлення й відновлення втрачених пакетів, зокрема алгоритмів повторного передавання та алгоритмів виявлення дублікатів;

– підтримує контроль потоку на рівні каналів і потоків.

RUDP:

– містить механізми виявлення й відновлення втрачених пакетів, подібно до TCP, але з меншою складністю;

– може мати механізми контролю потоку, хоча конкретна реалізація може варіюватися залежно від використовуваної бібліотеки чи програмного забезпечення.

Протокол RUDP не відповідає вимогам стандартизації.

Розглянемо протоколи TCP, MPTCP, SCTP з точки зору захищеності.

Протокол TCP має низку вразливостей до сучасних типів атак. Недоліки протоколу виявляються в успішних теоретичних і практичних атаках, у яких зловмисник може отримати доступ до переданих даних, видати себе за іншу сторону чи привести систему у неробочий стан. Прикладами цих атак є такі, як TCP Hijacking та TCP Reset.

Незважаючи на низку очевидних переваг Multipath TCP перед своїм попередником, цей протокол створює нові проблеми. З точки зору безпеки мережі, багатошляхова маршрутизація спричиняє перехресну фрагментацію даних, що призводить до того, що брандмауери та сканери шкідливих програм стають неефективними, коли вони бачать трафік лише одного шляху. Крім того, розшифровка SSL стане неефективною через протоколи наскрізного шифрування.

SCTP був розроблений з деякими функціями, що дозволяють підвищити безпеку, такими як “4-кратне рукостискання” (порівняно з “трикратним рукостисканням” у TCP), щоб запобігти SYN-flood атакам, і великим Cookie для перевірки справжності асоціації. Надійність була одним із ключових аспектів розроблення безпеки протоколу SCTP. Multi-homing дозволяє асоціації залишатися відкритою, навіть якщо деякі маршрути та інтерфейси, що використовуються, стали недоступні. Це дає можливість досягти стійкості під час короткострокових відключень зв’язків для підтримки телекомунікаційних послуг, навіть у разі

серйозних аномалій у мережі. Є захист від DDoS-атак. Шифрування не є частиною оригінального дизайну SCTP.

Хоча SCTP має деякі методи захисту, він не має такого рівня підтримки та екосистеми для безпеки, як TCP. Але слід зазначити, що, на відміну від TCP, немає загальновідомих фактів успішних атак на інфраструктури, що використовують протокол передавання даних SCTP. Варто також зауважити, що у разі використання протоколу Transport Layer Security (TLS) (укр. Протокол захисту транспортного рівня) у зв'язці з SCTP можна досягти достатньо високого рівня захищеності інформації під час передавання.

Дослідивши протокол SCTP на відповідність іншим вимогам, що висуваються для протоколів передавання даних у перспективній автоматизованій системі обміну науковою (науково-технічною) інформацією у ЗС України, а саме: багатопоточність, контроль потоків даних, стійкість до відмов, підтримка використовуваних у ЗС України операційних систем, можна стверджувати, що Stream Control Transmission Protocol у повній мірі відповідає їм (RFC4960, 2015; Seggelmann, 2012).

Обговорення (Discussions)

Аналізуючи останні публікації у сфері досліджень протоколів передавання даних транспортного та інших рівнів мережних моделей (Костюк, 2021; Іванчук, 2020; Малохвій, 2022; Жихарєв, 2022; Світличний, 2018; Chaudhari, 2018; Кравченко, 2020; Москвін, 2022), можна дійти таких висновків:

– загалом розглядаються тільки найчастіше використовувані протоколи, деякі з них – застарілі та вразливі до сучасних атак;

– аналіз проводиться на основі одного з параметрів протоколів, не розглядаються характеристики в комплексі та не враховуються недоліки і переваги кожного протоколу, відповідно до поставленого завдання;

– дослідження базуються на розгляді протоколів вищих рівнів мережних моделей;

– недостатньо інформації щодо застосування новітніх технологій у сфері забезпечення функціонування освітніх та наукових систем;

– науковцями Російської Федерації розглядається застосування більш сучасних технологій передавання даних у своїх автоматизованих системах (у тому числі військового спрямування) на противагу застарілим вітчизняним системам.

Таким чином, через недостатню кількість досліджень у сфері використання протоколів передавання даних у автоматизованих системах обміну інформацією не можна дати ґрунтовну відповідь про раціональність використання того чи іншого інструменту у визначених системах. Потреба у сучасних та захищених способах обміну інформацією зумовлює необхідність проведення аналізу цієї галузі, з визначенням та поясненням ролі протоколів, що можуть застосовуватися для передавання даних у перспективній автоматизованій системі обміну науковою (науково-технічною) інформацією у ЗС України.

Висновки (Conclusion)

Забезпеченням надійності інформаційного зв'язку між двома кінцевими вузлами займається транспортний рівень, а стек протоколів TCP/IP надає транспортні послуги прикладним процесам. Транспортні послуги цих протоколів мають відмінності.

Серед проаналізованих протоколів протокол SCTP виділяється своєю масштабованістю, надійністю, підтримкою безпеки та іншими функціями. Це робить його кращим варіантом для сучасних мереж і додатків, особливо в ситуаціях, коли важливе безперебійне передавання інформації.

Таким чином, відповідно до вказаних вище функцій заданої системи, використання протоколу SCTP більш доцільне для обміну науковою (науково-технічною) інформацією.

Перспектива подальших досліджень вбачається в аналізі доцільності використання новітніх протоколів передавання даних Tachyon, FASP та визначення їхньої взаємосумісності з іншими існуючими протоколами передавання даних для використання їх у автоматизованій системі обміну науковою (науково-технічною) інформацією.

Рекомендації (Recommendations)

Результати вищенаведеного матеріалу можуть бути корисні дослідникам, що займаються питаннями опису та створення автоматизованих систем військового призначення.

Використані джерела

1. Papastergiou Giorgos; Fairhurst Gorry; Ros David; Brunstrom Anna; Grinnemo Karl-Johan; Hurtig Per; Khademi Naeem; Tüxen Michael; Welzl Michael; Damjanovic Dragana; Mangiante Simone (2017). De-Ossifying the Internet Transport Layer: A Survey and Future Perspectives. IEEE Communications Surveys & Tutorials. 19: С. 619–639.
2. Computer networking: a top-down approach. James F. Kurose, University of Massachusetts, Amherst, Keith W. Ross, NYU and NYU Shanghai. Seventh edition. Hoboken, New Jersey. Pearson. 2017.
3. Reference Implementation for SCTP – RFC4960. – «This is the reference implementation for SCTP. It is portable and runs on FreeBSD/MAC-OS/Windows and in User Space (including linux).». URL: https://github.com/sctplab/sctp-refimpl.
4. Seggelmann R.; Tuxen M.; Rathgeb E. P. SSH over SCTP – Optimizing a multi-channel protocol by adapting it to SCTP. Communication Systems, Networks & Digital Signal Processing (CSNDSP). 8th International Symposium on: journal. 2012. 18 July. P. 1–6. ISBN 978-1-4577-1473-3.
5. Kostjuk Ju., Shestak Ja. Transportnyj riven'modeli ISO/OSI v komp’juternyh merezhah. Tovary i rynky. Mizhnarodnyj naukovo-praktychnyj zhurnal. 2021. № 4. P. 49–58.
6. Іванчук О. В., Завгородній В. В., Козел В. М., Дроздова Є. А. Аналіз протоколів обміну даними для керування системами інтернету речей. Вчені записки Таврійського Національного Університету ім. В. І. Вернадського. Серія: Технічні науки. Том 31 (70). Ч. 1. 2020. № 2 . С. 99–104.
7. Малохвій Е. Е., Молчанов Г. І., Паржин Ю. В. Дослідження протоколів передачі даних в умовах Інтернету речей. Системи управління, навігації та зв’язку. Зб. наук. пр. Вип. 1 (67). 2022. С. 71–74.
8. Жихарев А. Г., Фефелов О. С., Маматов М. Е. Обзор некоторых протоколов передачи данных с позиции их безопасности. Научный результат. Информ. технологии. Т. 7. 2022. № 1. С. 27–31.
9. Світличний В. А., Онищенко Ю. М. Протоколи, методи і технології захисту комп’ютерних мереж на транспортному рівні. Актуальні питання протидії кіберзлочинності та торгівлі людьми (м. Харків. 23 лист. 2018 р.). Харків. ХНУВС. 2018. С. 308–311.
10. Chaudhari, Ketulkumar Govindbhai. Analysis on Transport Layer Protocols and Its Developments (2018). International Journal of Innovative Research in Computer and Communication Engineering. 6(9). 7707–7712. Available at SSRN: https://ssrn.com/abstract=3729064 or http://dx.doi.org/10.2139/ssrn.3729064
11. Кравченко М. В., Никитин А. С., Спиридонов С. И. Об унификации обмена данными между разнородными средствами и системами в едином информационном пространстве. I-methods. 2020. № 2.

12. Москвин А. А. Технологии многопоточной передачи данных в информационных системах. Материалы XXII Междунар. научно-практ. конф. им. Э. К. Алгазинова. Под ред. Д. Н. Борисова. Воронеж. 2022. С. 688–696.

References

1. Papastergiou Giorgos; Fairhurst Gorry; Ross David; Brunstrom Anna; Grinnemo Karl-Johan; Hurtig Per; Khademi Naeem; Tüxen Michael; Welzl Michael; Dragana Damjanovic; Mangiante Simone (2017). De-Ossifying the Internet Transport Layer: A Survey and Future Perspectives. IEEE Communications Surveys & Tutorials. 19: pp. 619–639.
2. Computer networking: a top-down approach. James F. Kurose, University of Massachusetts, Amherst, Keith W. Ross, NYU and NYU Shanghai. Seventh edition. Hoboken, New Jersey. Pearson. 2017.
3. Reference Implementation for SCTP - RFC4960. - "This is the reference implementation for SCTP. It is portable and runs on FreeBSD/MAC-OS/Windows and in User Space (includinglinux).». URL: https://github.com/sctplab/sctp-refimpl.
4. Seggelmann R.; Tuxen M.; Rathgeb EP SSH over SCTP – Optimizing a multi-channel protocol by adapting it to SCTP. Communication Systems, Networks & Digital Signal Processing (CSNDSP). 8th International Symposium on: journal. 2012. 18 July. P. 1–6. ISBN 978-1-4577-1473-3.
5. Kostjuk Ju., Shestak Ja. Transportnyj riven'modeli ISO/OSI v komp'juternyh merezhah. Tovary i rynky. Mizhnarodnyj naukovo-praktychnyj zhurnal. 2021. No. 4. P. 49–58.
6. Ivanchuk O., Zavhorodniy V., Kozel V., Drozdova E. Analysis of data exchange protocols for managing Internet of Things systems. Scientific notes of the Tavriiski National University named after V. Vernadskyi. Series: Technical sciences. Volume 31 (70). Part 1. 2020. No. 2. P. 99–104.
7. Malochvii E., Molchanov G., Parzhin Yu. Research of data transfer protocols in the conditions of the Internet of Things. Management, navigation and communication systems. Coll. of science Ave. Issue 1 (67). 2022. P. 71–74.
8. Zhikharev A., Fefelov O., Mamatov M. Overview of some data transfer protocols from the perspective of their security. Scientific result. Information technologies. Vol. 7. 2022. No. 1. P. 27–31.
9. Svitlichny V., Onyshchenko Yu. Protocols, methods and technologies for protecting computer networks at the transport level. Actual issues of combating cybercrime and human trafficking (Kharkov, November 23, 2018). Kharkiv. KhNUAF 2018. P. 308–311.
10. Chaudhari, Ketulkumar Govindbhai. Analysis on Transport Layer Protocols and Its Developments (2018). International Journal of Innovative Research in Computer and Communication Engineering. 6(9). 7707–7712. Available at SSRN: https://ssrn.com/abstract=3729064 or http://dx.doi.org/10.2139/ssrn.3729064
11. Kravchenko M., Nikityn A., Spiridonov S. On the unification of data exchange between heterogeneous means and systems in a single information space. I-methods. 2020. No. 2.
12. Moskvin A. Technologies of multithreaded data transfer in information systems. Materials XXII International scientific and practical conf. named after E. Algazinova. Ed. D. Borisov. Voronezh. 2022. P. 688–696.

The data transfer protocols analysis in the perspective scientific (scientific and technical) information exchange automated system in the Armed Forces of Ukraine

Oleksii Nozdrachov
deputy head of the institute for moral and psychological support
Central Research Institute of the Armed Forces of Ukraine
03049, 28B, ave. Povitroflotskyi, Kyiv, Ukraine
e-mail: o.o.nozdrachov@post.mil.gov.ua

Mykola Vasianovych
candidate of military sciences, senior researcher
head of the center
Central Research Institute of the Armed Forces of Ukraine
03049, 28B, ave. Povitroflotskyi, Kyiv, Ukraine
e-mail: m.o.vasianovych@post.mil.gov.ua
ORCID: 0000-0002-8409-4774

Andrii Shnukalo
Senior Research Fellow
Central Research Institute of the Armed Forces of Ukraine
03049, 28B, ave. Povitroflotskyi, Kyiv, Ukraine
e-mail: a.d.shnukalo@post.mil.gov.ua
ORCID: 0000-0002-1205-9953

Abstract. The relevance of the study is due to the need to define effective data transfer protocols that ensure high quality of service and security of automated information exchange systems in the Armed Forces of Ukraine and their components.

In this regard, the article is aimed at revealing the protocols of the transport level of the TCP/IP and OSI network models - User Datagram Protocol, User Datagram Protocol Lite, Transmission Control Protocol, Multipath Transmission Control Protocol, Stream Control Transmission Protocol, Datagram Congestion Control Protocol, Reliable User Datagram Protocol from the perspective of their application point of view in the automated systems of scientific (scientific and technical) information exchange in the Armed Forces of Ukraine.

The leading approaches to the study of this problem are the use of informational and logical analysis methods, which allow a comprehensive consideration of network models by means of comparison.

About 15 characteristics has been considered, in particular: transmission reliability, overload control, multithreading. Taking into account the requirements and features of the promising automated system of scientific (scientific and technical) information exchange in the Armed Forces of Ukraine, it was proposed to use certain technological combinations with higher-level protocols to achieve optimal data protection. As a result of the analysis, it was established that, in accordance with the functions of the automated exchange of scientific (scientific and technical) information system, it is more expedient to use the Stream Control Transmission Protocol.

The materials of the article are of a theoretical value for conducting further scientific research on the problem raised, as well as practical value for the improvement of military information systems, in accordance with the standards of the North Atlantic Alliance and today's challenges in cyberspace.

Keywords: data exchange, information technologies, network technologies, military-scientific automated systems.