УДК 621.81:621.253.2

МОДИФІКАЦІЯ NTP СЕРВЕРА ЧАСУ СИСТЕМИ ДИФЕРЕНЦІАЛЬНОЇ КОРЕКЦІЇ ВІДПОВІДНО ДО СХЕМИ ANSI X9.95

В.В. Солдатов[1], О. П. Нарєжній[2], Т.О. Гріненко[3]

[1]*Національний науковий центр "Інститут метрології", вул. Мироносицька, 42, 61002, Харків, Україна time.metrology@ukr.net*
[2]*Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, 61000, Харків, Україна, o.nariezhnii@karazin.ua*
[3]*Харківський національний університет радіоелектроніки, просп. Науки, 14, 61166, Харків, Україна, tetiana.grinenko@nure.ua*

Анотація

В роботі розглядаються метрологічні аспекти побудови макета NTP сервера, призначеного для застосування в автономній системі диференціальної корекції (СДК). Показано, що навмисне перекручування даних вектора стану сигналу GPS / GLONASS і диференціальних поправок контрольно-коригувальних станцій (ККС) є основним завданням кібератаки на алгоритми A-GPS або GPS мобільних пристроїв (смартфонів). Даний тип хакерської атаки відноситься до атак модифікації. Для усунення загрози порушення цілісності диференціальних поправок застосовується процедура автентифікації коригувальної інформації (КІ), що транслюється ККС. При цьому здійснюється перевірка даних, що передаються ККС, на предмет модифікації, порядку проходження і своєчасності доставки повідомлень КІ. Процес автентифікації трансльованих повідомлень передбачає приєднання до КІ блоку даних фіксованого розміру, що є кодом автентифікації повідомлення (Message Authentication Code, MAC). Передбачається, що дві сторони, які беруть участь в обміні даних, ККС і мобільний пристрій користувача, використовують загальний поточний MAC і довірчу мітку часу NTP сервера. Основне завдання NTP сервера полягає в незалежній синхронізації передачі КІ і формуванні поточного MAC. Для формування поточного MAC застосовується модифікований код поточного значення часу NTP сервера відповідно до схеми X9.95.

Ключові слова: NTP сервера; GPS / GLONASS; кібератаки на алгоритми A-GPS / GPS; процедура автентифікації; Message Authentication Code.

Вступ

Служба єдиного часу і еталонних частот (СЄЧЧ) здійснює міжгалузеву координацію та виконання робіт, спрямованих на забезпечення єдності вимірювань часу і частоти та визначення параметрів обертання Землі та надання часо-частотної інформації споживачам в економіці, у сфері науки та оборони, а також фізичним та юридичним особам, у тому числі надання інформації для забезпечення застосування єдиного обліково-звітного часу [1,2]. Основним завданням СЄЧЧ є забезпечення єдності вимірювань часу і частоти та синхронної роботи технічних засобів державної мережі моніторингу глобальних навігаційних супутникових систем (ГНСС) з державним еталоном часу і частоти [3].

Вирішення вказаних завдань пропонується здійснювати методами диференціальної корекції за рахунок введення різного роду поправок до навігаційних радіосигналів відкритого доступу ГНСС типу GPS/GLONASS. Це дозволить забезпечити споживачів навігаційними визначеннями GPS/GLONASS з сантиметровою точністю в реальному масштабі часу відносно національної шкали часу UTC(UA), що формується державним еталоном часу і частоти ДЕТУ 07-01-97.

В якості космічного доповнення даних ГНСС пропонується використовувати сигнали широкозонної СДК типу SBAS/EGNOS (ЄС). Космічні апарати (КА) EGNOS в діапазоні GPS L1(C/A) передають інформацію цілісності навігаційного поля і коригувальну інформацію (КІ). Данні КА широкозонної EGNOS, що знаходяться на геостаціонарній орбіті, забезпечують оперативну передачу всім споживачам України КІ такого складу: поправки до бортових ефемерид, частотно-часові поправки по кожному навігаційному КА GPS/GLONASS і GALILEO та поправки величин вертикальної іоносферної і тропосферної затримки.

Для вирішення завдань координатно-часового забезпечення України перспективну національну СДК доцільно будувати як систему, що розвивається та поетапно нарощується. На даному етапі необхідно об'єднати всі локальні мережі різних відомств, що складаються з декількох спільно працюючих контрольно-коригувальних станцій (ККС), координати яких відомі з високою точністю. Подальше розширення робочих зон пропонується здійснювати за рахунок спільної роботи в реальному часі групи мобільних ККС, одна з яких виконує функції провідної (стаціонарної) [4].

У ролі ведучих ККС пропонується використовувати мережу IGS на території України, що складається з стаціонарних станцій з номерами DOMES: 12314M001, 12356M001, 12335M001, 12366M001. Центр диференціальної корекції і моніторингу будується на базі стаціонарних станцій DOMES 12314M001, де розташований ДЕТУ 07-01-97.

В якості каналу доставки КІ авторизованим користувачам передбачається використовувати Internet протокол SISNet і NTRIP. Мобільні ККС компенсують іоносферну затримку двочастотним методом, а тропосферну затримку за допомогою комплексування моделі і КІ широкозонної EGNOS. В результаті спільної обробки мобільна ККС можезабезпечити вирішення неоднозначності фази

несучої L1(C/A) на відстанях до 250 км щодо провідної (стаціонарної) станції.

Для побудови підсистеми єдиного часу ведучих станцій (ККС) національної СДК пропонується використовувати протокол PTP на волоконно-оптичних лініях зв'язку рівня L2. Ведучі станції необхідно обладнати серверами точного часу PTP Microsemi Time Provider 4100, що синхронізуються цезієвим стандартом частоти Microsemi 5071A зі складу ДЕТУ 07-01-97 [5]. У мобільних ККС синхронізацію видачі КІ з національною шкалою часу UTC(UA) пропонується здійснювати за протоколом NTP v.4 [6,7].

Джерела КІ мають ряд вразливостей як по радіонавігаційному сигналу навігаційного КА, так і по каналу передачі поправок від ККС [4]. Також відомі і відпрацьовані атаки на GPS [8]. Крім того, сучасні сервера точного часу NTP, наприклад, Microsemi Time Provider 4100, використовують в протоколі автентифікації алгоритм 128-бітного гешування MD5 (Message Digest) [9]. З 2011 року відповідно до RFC 6151 алгоритм MD5 вважається ненадійнім [7, 9].

Задача щодо теоретичного обґрунтування і практичного застосування сучасних криптостійких MAC відповідно до схеми ANSI X9.95 має важливе практичне та наукове значення при розробці національної СДК.

Мета статті

Вирішення задачі усунення вразливості даних СДК в разі застосування MD5 в протоколі NTP. Модифікація NTP сервера часу СДК відповідно до схеми ANSI X9.95 з використанням криптографічно стійкої імітовставки (MAC). Метрологічне дослідження макету NTP сервера СДК з криптографічно стійкою MAC.

Виклад основного матеріалу

Як канал доставки довірчої мітки часу авторизованим користувачам СДК передбачається використовувати Internet. При цьому застосування сучасних систем шифрування для послуги конфіденційність у протоколі NTP визнано США забороненим в Internet [7].

Тому, по-перше, протоколи NTP версій 3 та 4 не включають сучасну криптографію (з точки зору урядових постанов США), а використовують тільки ключі імітовставки типу MD5. Тобто забезпечується реалізація послуги цілісності даних протоколу NTP, що не суперечить умовам застосовності мітки часу для синхронізації КІ в національній СДК.

По-друге, відомо, що реалізація MD5 має майже постійні часові цикли формування цифрового підпису. Для NTP серверів часу даний параметр є серйозною перевагою, що забезпечує необхідну навантажувальну здатність і похибку синхронізації. При цьому застосування алгоритмів з відкритим ключем потребує значної кількості непостійних в часі циклів цифрового підпису.

Схема ANSI X9.95 дозволяє в якості криптографічної контрольної суми для контролю цілісності даних NTP у захищеному з'єднанні використовувати MAC (імітовставку), яка обчислюється за алгоритмом блочного симетричного шифру (БСШ) згідно ДСТУ ГОСТ 28147:2009 або TDEA чи AES.

При цьому протокол NTP дозволяє застосовувати БСШ (імітовставка обмежена 128 бітами) тільки для перевірки цілісності й автентифікації (перевірка цілісності). Симетричні ключі (загальні секрети) використовуються для підтвердження справжності даних протоколу NTP. Механізм Autokey протоколу NTP дозволяє також використовувати пари ключів, отриманих по мережі Internet там, де складно встановити загальні секрети.

У протоколі застосовуються такі автентифіковані повідомлення: команди віддаленого налаштування і час повідомлення (автентифікація не обов'язкова).

Шифрування симетричним ключем вимагає наявність безпечного каналу в СДК для обміну секретними ключами. Кожен авторизований користувач NTP потребує секретний ключ для автентифікації повідомлень часу від сервера. Тому криптографія з відкритим ключем і сертифікати X.509 протоколу NTP версії 3 та 4 використовуються для нової схеми автентифікації СДК, яка узагальнена нижче.

Авторизовані користувачі СДК визначають підмножину мережі NTP, яка використовує загальну модель безпеки, протокол автентифікації і схему ідентифікації. Кожна ККС і авторизований користувач мають параметри автентифікації і груповий ключ, що надається деякою довіреною стороною (центром сертифікації ключів). У кожної захищеної групи користувачів є, принаймні, один довірений вузол мережі (host), який працює як центр сертифікації на найнижчому рівні групи. Первинна група ККС включає, щонайменше, один первинний сервер (stratum 1).

Схеми ідентифікації ККС в системі СДК побудовані на методах підтвердження ККС, що дозволяє запобігти атакам типу модифікація. Відомо, що в алгоритмах безпеки NTP і в моделі безпеки NTP використовуються такі схеми ідентифікації [7]:

приватний сертифікат PC (Private Certificate);

довірений сертифікат TC (Trusted Certificate);

схема ідентифікації IFF (Schnorr Identity Scheme);

схема ідентифікації GQ (Guillou-Quisquater Identity Scheme);

схема ідентифікації MV (Mu-Varadharajan Identity Scheme).

Схема PC вимагає секретного каналу для поширення закритих ключів. Схема TC використовує довірений орган (PKI) і ланцюжки сертифікатів. Схема IFF базується на DSA. Схема MV також базується на DSA, але не вимагає довірених клієнтів. Схема GQ базується на RSA.

Всі схеми використовують відносно невеликі ключі (128 біт), тому ці ключі повинні регулярно оновлюватися. При цьому сертифікати дійсні протягом одного року після створення, а ключі повинні генеруватися з більш короткими інтервалами. При цьому застосування мітки часу NTP як серійного номера сертифікатів повинно забезпечувати унікальність. Таким чином, підписи в СДК

генеруються тільки тоді, коли час вузла мережі (host) вважається синхронізованим.

Формати ключових даних та іншої спеціальної інформації СДК повинні відповідати вимогам міжнародних та національних стандартів, рекомендацій та діючих нормативних документів. Наприклад, формати запитів на формування позначок часу та самих позначок часу (протокол TSP) авторизованих користувачів повинні бути виконані згідно ДСТУ ETSI EN 319 422:2016 та технічних рекомендацій RFC 3161 [10, 11]

При цьому до складу криптографічного комплексу національної СДК необхідно включити:

апаратні засоби криптографічного захисту інформації (КЗІ);

програмні засоби (бібліотеки) КЗІ (користувача ЦСК) "ІІТ Користувач ЦСК-1" [12].

Апаратна реалізація КЗІ (електронний ключ) забезпечує захищеність процесу виконання криптографічних перетворень СДК та унеможливлює доступ до особистих ключів з боку апаратного-програмного середовища. Особисті ключі генеруються, зберігаються та використовуються тільки усередині електронного ключа, та жодним способом не потрапляють за його межі [12].

В макеті NTP серверів часу всіх рівнів використовуються апаратні засоби криптографічного захисту інформації. В якості носіїв ключової інформації для особистих ключів та криптомодулів може використовуватися електронний ключ “Кристал-1” (“ІІТ Е.ключ Кристал-1”) [12].

При цьому електронний ключ в макетах NTP серверів виконує наступні функції:

генерацію ключів для алгоритму БСШ на основі апаратного генератора;

зберігання особистих ключів у внутрішній пам'яті та захист їх від несанкціонованого доступу;

розподіл ключових даних на основі асиметричного протоколу розподілу.

Електронний ключ “Кристал-1” генерує імітовставку згідно ДСТУ ГОСТ 28147:2009, який з 2021 року є забороненим для застосування на території України. Тому для виробки імітовставки (MAC) застосовувалася програмна реалізація БСШ шифр Калина (англ. Kalyna), що описана у національному стандарті України ДСТУ 7624:2014 [13]. Даний алгоритм підтримує такі режими виробки імітовставки (режим CMAC) і вибіркове гамування із прискореним виробленням імітовставки (режим GMAC) та вироблення імітовставки і гамування (режим CCM). В макеті NTP сервера рис. 1 и рис. 2 при виробці MAC була апробована програмна реалізація режиму CCM блочного симетричного шифру з параметрами Kalyna-256/512-CCM-32,128 з довжиною імітовставки 128 бітів. Потенційним недоліком використання БСШ Kalyna-256/512-CCM-32,128 є обмеження навантажувальної здатності прототипу NTP сервера, що потребує подальших експериментальних досліджень.

До складу макету NTP сервера часу, що приведений на рис.1 та рис.2 входять:

приймач ГНСС NovAtel GPS Receiver (OEM6);

керуючій одноплатний комп'ютер Raspberry Pi 3;

рубідієвий стандарт частоти та часу PRS10;

приймальна антена ГНСС NovAtel NOV702GG.

Зовнішній вигляд експериментальної установки (первинної ККС) наведено на рис. 2. До складу первинної ККС входять:

приймальні антени GPS/GLONASS/EGNOS;

приймачі GPS/GLONASS та SBAS/EGNOS;

керуюча персональна обчислювальна машина;

сервер часу NTP (stratum 1) з автентифікацією MAC;

цезієвий стандарт частоти та часу зі складу ДЕТУ 07-01-97;

електронний ключ “Кристал-1”;

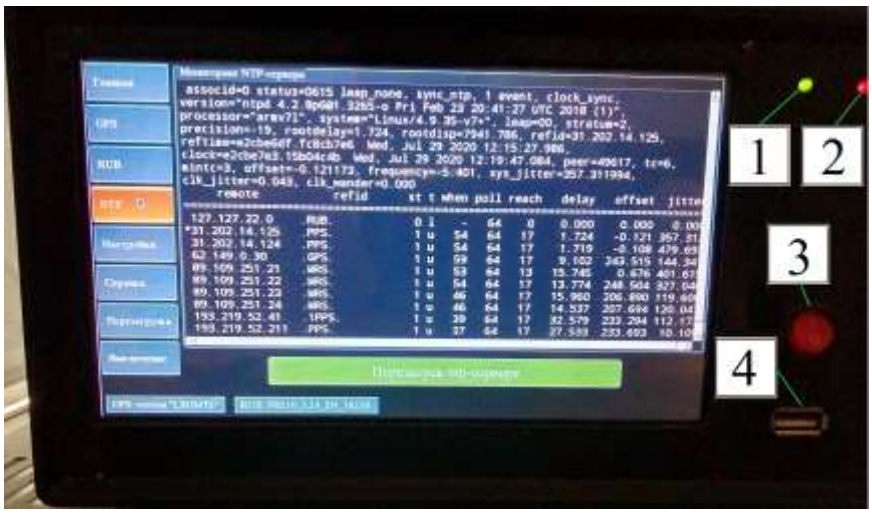
захищений канал обміну даних СДК з системою IGS (файли RINEX);

канал прийому даних від мережі ККС та ретрансляції КІ до споживачів.

1 – Прототип серверу часу NTP (stratum 1) з автентифікацією MAC

2 – Опорний цезієвий стандарт частот Microsemi 5071A зі складу ДЕТУ 07-01-97

Рис.1. Прототип серверу часу NTP (stratum 1) для центрального пункту управління СДК з автентифікацією MAC



1 – Індикатор синхронізації по GPS приймачу
2 – Індикатор зникнення мережі електропостачання і роботи від внутрішнього акумулятора
3 – відключення індикації сенсорного TFT LCD дисплею
4 – USB- з'єднувач для підключення електронного ключа "Кристал-1"
Рис.2. Прототип серверу часу NTP (stratum 2) для мобільної ККС з автентифікацією MAC

Висновки

Система СДК передбачає формування поправок безпосередньо до вектора-стану авторизованого споживача. Вектор-стану авторизованого споживача в системі WGS-84 складається з: вектора положення та швидкості споживача, поправки до частоти опорного генератора та поправки до шкали часу споживача. Даний варіант дозволяє послабити вплив повільнозмінних похибок спостережень, обумовлених, головним чином, впливом середовища розповсюдження радіохвиль. За результатами прийому і обробки навігаційних сигналів в апаратурі локальної ККС формується різниця між еталонним вектором стану ККС та вектор-стану споживача в реальному часі UTC(UA). Вектор стану ККС в системі WGS-84, а саме складові вектора швидкості антени станції дорівнюють нулю, що оцінюється у процесі розв'язання навігаційно-часової задачі.

Недолік такого формування поправок обумовлений тим, що вектори стану, як правило, спостерігаються за різними сузір'ями навігаційних КА. Моделювання різниць векторів-стану, що синхронізувались відповідно до схеми ANSI X9.95 з використанням криптографічно стійкої імітовставки, що формувалася з використанням шифру Kalyna-256/512-CCM-32,128, показали наявність обмежень на навантажувальну спроможність не більше 100 локальних і стаціонарних ККС в національній СДК.

Abstract

The paper discusses the metrological aspects of building a model of an NTP server intended for use in an autonomous differential correction system (SDK). It is shown that the deliberate distortion of the data of the GPS / GLONASS signal state vector and differential corrections of control and correcting stations (CCS) is the main task of a cyberattack on A-GPS or GPS algorithms of mobile devices (smartphones). This type of hacker attack belongs to modification attacks. To eliminate the threat of violation of the integrity of differential corrections, the procedure for authenticating the correcting information (CI) transmitted by the CCS is applied. At the same time, the transmitted KKS data is checked for modification, the order of passage and the timeliness of delivery of KI messages. The process of authenticating broadcast messages involves attaching a fixed-size data block called a Message Authentication Code (MAC) to the CI. It is assumed that the two parties involved in the exchange of data, the KKS and the user's mobile device, use a common current MAC and NTP server trust timestamp. The main task of the NTP server is to independently synchronize the transfer of information and the formation of the current MAC. To form the current MAC, the modified code of the current value of the NTP server time is used in accordance with the X9.95 scheme.

Key words: NTP server; GPS / GLONASS; cyber attacks on A-GPS / GPS algorithms; authentication procedure.

Аннотация

В работе рассматриваются метрологические аспекты построения макета NTP сервера, предназначенного для применения в автономной системе дифференциальной коррекции (СДК). Показано, что умышленное искажение данных вектора состояния сигнала GPS/GLONASS и дифференциальных поправок контрольно-корректирующих станций (ККС) является основной задачей кибератаки на алгоритмы A-GPS или GPS мобильных устройств (смартфонов). Данный тип хакерской атаки относится к атакам модификации. Для устранения угрозы нарушения целостности дифференциальных поправок применяется процедура аутентификации корректирующей информации (КИ) транслируемой ККС. При этом осуществляется проверка передаваемых данных ККС на предмет модификации, порядка прохождения и своевременности доставки сообщений КИ. Процесс аутентификации транслируемых сообщений предполагает присоединение к КИ блока данных фиксированного размера, называемого кодом аутентификации сообщения (Message Authentication Code, MAC).

Предполагается, что две стороны, участвующие в обмене данных, ККС и мобильное устройство пользователя, используют общий текущий МАС и доверительную метку времени NTP сервера. Основная задача NTP сервера состоит в независимой синхронизации передачи КИ и формирования, текущего МАС. Для формирования, текущего МАС применяется модифицированный код текущего значения времени NTP сервера в соответствии со схемой X9.95.

Ключевые слова: NTP сервер; GPS / GLONASS; кибератаки на алгоритмы A-GPS/GPS; процедура аутентификации; Message Authentication Code.

Список літератури

1. Про метрологію та метрологічну діяльність [Електронний ресурс] : закон України від 03.07.2019р. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1314-18. – (дата звернення 25.05.2020).
2. Положення про Службу єдиного часу і еталонних частот [Електронний ресурс] : постанова Кабінету Міністрів України № 664 від 2.09.2015 р. – Режим доступу : https://zakon.rada.gov.ua/laws/show/664-2015-n. – (дата звернення 25.05.2020).
3. Про утворення державної мережі моніторингу глобальних навігаційних супутникових систем [Електронний ресурс] : постанова Кабінету Міністрів України № 486 від 7.04.2003 р. – Режим доступу : https://zakon.rada.gov.ua/laws/show/486-2003-n. – (дата звернення 25.05.2020).
4. Т.А. Гриненко, А.П. Нарежний. Применение кодов аутентификации сообщений для обнаружения модификаций данных в региональных системах дифференциальной коррекции навигационных сигналов систем GPS/ГЛОНАСС. *Прикладная радиоэлектроника*, 2014. Т.13. № 3. С. 301–310.
5. Солдатов В.В., Дзисюк О.В., Бойко В.М., Гаврилов А.Б., Свiтенко М.І., Рарог Р.М., Свистун А.М., Матвієнко М.В. Результати дослідної експлуатації підсистеми забезпечення єдиним часом військових споживачів на базі серверів точного часу Microsemi Time Provider 4100. *Український метрологічний журнал,* 2020. № 1. С. 68-78 doi: 10.24027/2306-7039.1.2020.204255
6. IETF RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification" Available at: https://tools.ietf.org/html/rfc5905 (accessed 25.05.2020).
7. IETF RFC 5906: "Network Time Protocol Version 4: Autokey Specification". Available at: https://tools.ietf.org/html/rfc5906 (accessed 25.05.2020).
8. Tippenhauer N., Pöpper C., Rasmussen K., Capkun S. On the requirements for successful GPS spoofing attacks. Proceedings of the 18th ACM *Conference on Computer and Communications Security* (CCS'11). Chicago. Illinois. 2011. P. 75–86.
9. IETF RFC 6151: "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms" Available at: https://tools.ietf.org/html/rfc6151 (accessed 25.05.2020).
10. ДСТУ ETSI EN 319 422:2016 IDT. Електронні підписи та інфраструктури. Протокол мітки часу та профілі токенів мітки часу. Київ: Держстандарт України, 2016. 14 р.
11. IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)". Available at: https://tools.ietf.org/html/rfc3161 (accessed 25.05.2020).
12. ІІТ Е.ключ Кристал-1. : веб-сайт. URL: https://iit.com.ua/index.php?page=itemdetails&p=3&gtype=1&type=1&id=50 (дата звернення: 25.05.2020).
13. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. Київ: Мінекономрозвитку України, 2016. 228 с.
14. Об Основных направлениях (плане) развития радионавигации государств – участников СНГ на 2019–2024 годы.

References

1. Pro metrolohiiu ta metrolohichnu diialnist [Elektronnyi resurs] : zakon Ukrainy vid 03.07.2019 r. – Available at: https://zakon.rada.gov.ua/laws/show/1314-18. – (accessed 25.05.2020).
2. Polozhennia pro Sluzhbu yedynoho chasu i etalonnykh chastot [Elektronnyi resurs] : postanova Kabinetu Ministriv Ukrainy № 664 vid 2.09.2015 r. – Available at: https://zakon.rada.gov.ua/laws/show/664-2015-n. – (accessed 25.05.2020).
3. Pro utvorennia derzhavnoi merezhi monitorynhu hlobalnykh navihatsiinykh suputnykovykh system [Elektronnyi resurs] : postanova Kabinetu Ministriv Ukrainy № 486 vid 7.04.2003 r. – Available at: https://zakon.rada.gov.ua/laws/show/486-2003-n. – (дата звернення 25.05.2020).
4. Grinenko T.O., Narezhniy O.P. Message authentication codes application for data modification detection in regional systems of differential correction of GPS/GLONASS systems navigation signals. *Applied Radio Electronics*: Sci. Journ. 2014. Vol. 13. № 3. P. 301–310
5. Soldatov V.V., Dzysiuk O.M., Bojko V.B., Gavrilov A.B., Svitenko M.I., Rarog R.M., Svystun A.M., Matvienko M.V. The results of pilot operation of the subsystem of universal time provision for military consumers based on the precise time servers Microsemi Time Provider 4100. *Ukrainian Metrological Journal*, 2020, no. 1. pp. 68–78 (in Ukrainian). doi: 10.24027/2306-7039.1.2020.204255
6. IETF RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification" Available at: https://tools.ietf.org/html/rfc5905 (accessed 25.05.2020).
7. IETF RFC 5906: "Network Time Protocol Version 4: Autokey Specification". Available at: https://tools.ietf.org/html/rfc5906 (accessed 25.05.2020).
8. Tippenhauer N., Pöpper C., Rasmussen K., Capkun S. On the requirements for successful GPS spoofing attacks/ Proceedings of the 18th ACM *Conference on Computer and Communications Security* (CCS'11). Chicago. Illinois. 2011. P. 75–86.
9. IETF RFC 6151: "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms" Available at: https://tools.ietf.org/html/rfc6151 (accessed 25.05.2020).
10. State Standard ETSI EN 319 422:2016 (ETSI EN 319 422:2016, IDT) Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles. Kyiv, Derzhstandart Ukrainy, 2016. 14 p. (in Ukrainian).
11. IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)". Available at: https://tools.ietf.org/html/rfc3161 (accessed 25.05.2020).
12. IIT E.ключ Кристал-1. Available at: https://iit.com.ua/index.php?page=itemdetails&p=3&gtype=1&type=1&id=50 (accessed 25.05.2020).
13. State Standard 7624:2014. Information Technology. Cryptographic protection of information. Symmetric block transformation algorithm. – Kyiv, Minekonomrozvytku Ukrainy, 2016. 228 p. (in Ukrainian).
14. About the Main directions (plan) of radio navigation development of the CIS member states for 2019-2024