УДК 621.317.76.089.68:621.373.82

ПРИМЕНЕНИЕ КОДОВ АУТЕНТИФИКАЦИИ СООБЩЕНИЙ ДЛЯ ОБНАРУЖЕНИЯ МОДИФИКАЦИЙ ДАННЫХ В РЕГИОНАЛЬНЫХ СИСТЕМАХ ДИФФЕРЕНЦИАЛЬНОЙ КОРРЕКЦИИ НАВИГАЦИОННЫХ СИГНАЛОВ СИСТЕМ GPS/ГЛОНАСС

Т.А. ГРИНЕНКО, А.П. НАРЕЖНИЙ

В данной статье обосновывается необходимость применения кодов аутентификации сообщений (MAC) для обеспечения целостности и достоверности корректирующей информации, формируемой системами дифференциальной коррекции навигационных сигналов систем GPS/ГЛОНАСС. На примере работы типовой схемы контрольно-корректирующей станции обосновывается необходимость применения MAC – алгоритмов при передаче «сырых» измерений уточненных эфемерид и частотно-временных поправок навигационно-космических аппаратов глобальных навигационных спутниковых систем GPS/ГЛОНАСС.

Ключевые слова: контрольно-корректирующая станция, защита данных, криптография, коды аутентификации сообщений.

ВВЕДЕНИЕ

Постановка проблемы. Современная система координатно-временного и навигационного обеспечения Украины строится на использовании радионавигационного поля глобальных навигационных спутниковых систем (ГНСС) GPS (США) и ГЛОНАСС (Российская Федерация), а также корректирующей информации (КИ) Европейской спутниковой системы дифференциальной коррекции (СДК) типа EGNOS (European Geostationary Navigation Overlay Service) [1]. Вместе с тем владельцами ГНСС являются военные ведомства данных стран, которые не исключают введение селективного доступа (Selective Availability, SA) к радионавигационным сигналам. Для повышения точности позиционирования и устранения влияния режима SA в мире строятся различные СДК. Поэтому для решения целого ряда задач экономики, безопасности и обороны в Украине разрабатывается ряд проектов, направленных на построение национальной СДК радионавигационных сигналов GPS/ГЛОНАСС [2].

Обеспечение аутентичности КИ радионавигационного поля ГНСС является одной из основных проблем, которые возникают перед разработчиками современных автоматизированных СДК. Актуальной эта проблема стала и для разработчиков функционального дополнения ГЛОНАСС в рамках развития проекта российской системы дифференциальной коррекции и мониторинга [3]. В результате был разработан Национальный стандарт Российской Федерации ГОСТ Р 54459-2011, который описывает общетехнические требования к СДК и обязывает разработчиков применять в аппаратно-программных комплексах данной системы средства защиты информации, передаваемой по общедоступным каналам связи [4].

Анализ литературы. В конце 2012 года исследователи из Университета Карнеги-Меллон и компании Coherent Navigation классифицировали новые типы уязвимостей системы GPS и оценили масштаб связанных с ними угроз [5]. В работе [5] описано несколько техник атаки на инфраструктуру системы GPS. Эта атака отличается от традиционных методов джамминга и спуфинга большим масштабом и представлением информационной системы GPS как компьютерной сети. В эксперименте по тестированию нового метода спуфинга были задействованы контрольные сообщения протокола GPS (в первом методе), особенности программного стека GPS (во втором методе) и программного обеспечения GPS-приёмников (третий метод).

Используя относительно простую аппаратно-программную систему, собранную из доступных на рынке недорогостоящих элементов, эти специалисты провели несколько новых концептуальных атак на GPS-устройства. При этом применялись следующие приёмы: фальсификация эфемерид GPS-спутников; передача некорректной информации о текущей дате; намеренная рассинхронизация шкал времени (ШВ); атака на системное программное обеспечение устройства (вторжение, повышение привилегий в системе); дезориентирующее искажение сигнала – псевдослучайного кода (спуфинг).

Атака апробирована на GPS-приёмниках семи производителей, включая Magellan, Garmin, GlobalSat, uBlox, LOCOSYS и iFly 700. Подобные устройства используются в легковых и грузовых автомобилях, самолётах, беспилотных летательных аппаратах, кораблях, станциях сотовой связи, в системах диспетчерского управления и сбора данных типа SCADA (Supervisory Control And Data Acquisition) и т.д. [6,7].

Кроме того, в работе [5] показано, что в результате 45-секундной сессии можно вывести из строя до 30% станций CORS (Continuously Operating Reference Stations) системы GPS и до 20% сетей, использующих протокол NTRIP

(Networked Transport of RTCM via Internet Protocol) [8].

Сеть станций CORS является аналогом региональной СДК, т. к. используется для ретрансляции данных ГНСС преимущественно на территории США, а сети с протоколом NTRIP передают данные системы GPS в онлайне. Исследователи показали, что многие коммерческие GPS-приёмники полагаются на эти данные, но из-за отсутствия криптографических методов проверки подлинности GPS-пакетов в коммерческих приложениях эти GPS-приёмники уязвимы к атакам. Для GPS-приёмников военного назначения, в которых используется криптографическая защита передаваемых данных, предлагаемый метод атаки [5] не работает.

На международной конференция ZeroNights 2012 года участник конференции, кандидат наук по безопасности встроенных устройств из университета EURECOM, Андрей Костин сообщил об уязвимости GPS системы наблюдения воздушного потока, экспериментально подтвердив возможность модифицировать данные сигналов протокола ADS-B (система наблюдения воздушного потока, которую диспетчеры и пилоты используют для отслеживания местонахождения самолетов, а также передачи важных данных и параметров). Как оказалось, протокол не использует никаких средств защиты при передаче данных, например, шифрования или электронной цифровой подписи [9]. Это позволяет отслеживать все самолеты в режиме реального времени и, самое главное, посылать в эфир поддельные данные или подменивать данные в настоящих пакетах, чтобы, например, сымитировать на экранах контролеров полетов воздушное столкновение самолетов.

Известно [10], что в среде Internet КИ от контрольно-корректирующей станции в СДК к потребителям в реальном времени доставляется в формате RTCM SC-104 (версия 2.2 и выше). Для этого применяют два протокола: SISNet и NTRIP [11]. Например, SISNet используют для распространения КИ, формируемой системой EGNOS. Протокол NTRIP применяют в функциональном дополнении ГНСС ГЛОНАСС – Российской системы дифференциальной коррекции и мониторинга [4, 12].

Перехват и модификация КИ в формате RTCM в Internet среде начинает принимать массовый характер. Согласно исследованиям [6,7], информация с недорогих встроенных в смартфон устройств геопозиционирования или персональных GPS-устройств, отслеживающих местонахождение потребителя, может с лёгкостью быть перехвачена хакерами, которые потом могут точно определить местонахождение устройства, выдать его за другой объект или подделать информацию о его физическом местонахождении.

Между тем, принято считать, что вероятность хакерской атаки на локальные ККС из состава национальной системы СДК незначительна, т. к. для реализации атаки необходимо применять дорогостоящие эталонные комплексы. Вследствие этого в Украине при разработке проектов региональных и ведомственных СДК вопросы защиты информации не рассматриваются. Наряду с этим не учитывается, что для обеспечения информационного взаимодействия в СДК будет использоваться Internet, т. к. в стране отсутствуют национальные системы передачи КИ [11].

В настоящее время вся информация о «сырых» измерениях уточненных эфемерид и частотно-временных поправок навигационного космического аппарата (НКА) систем GPS/ГЛОНАСС, полученная национальными ККС, передается в открытом виде. Вследствие этого существует реальная опасность хакерских атак на локальные ККС из состава национальной СДК. Поэтому применение криптографической защиты данных в СДК с целью повышения их стойкости и надежности является актуальной научно-технической задачей.

Цель статьи. Обоснование необходимости применения МАС кодов для обеспечения целостности и достоверности КИ в национальной СДК ГНСС GPS/ГЛОНАСС. Предлагается использовать МАС коды для выявления несанкционированных модификаций «сырых» данных, передаваемых пользователям ГНСС, как в зоне отдельно действующего пункта контроля, так и в зоне действия всей СДК в целом.

ОСНОВНАЯ ЧАСТЬ

Дифференциальный режим измерений основывается на пространственно-временной корреляции основных погрешностей измерений в навигационной аппаратуре потребителей (НАП) и в опорной точке Земной поверхности, где устанавливается контрольно-корректирующая станция (ККС). Математическая постановка задачи дифференциального режима измерений состоит в следующем. Вектор состояния ККС в общем случае имеет следующий вид

$$\vec{\lambda}_k = \left[x, y, z, \Delta T_k, \Delta_{0 f_k} \right],$$

где (x, y, z) – точные координаты локальной (мобильной) ККС в системах геодезических параметров Земли ПЗ-90 или WGS–84; ΔT_k – отклонение ШВ системы GPS от национальной координированной шкалы UTC(UA) в k-й момент времени передачи КИ; $\Delta_{0 f_k}$– относительное отклонение частоты опорного генератора в k-й момент времени передачи КИ.

Погрешность определения координат для ККС задается следующими соотношениями:

$$\Delta x_0 \in N\left(0, \sigma^2_{\Delta x}\right), \Delta y_0 \in N\left(0, \sigma^2_{\Delta y}\right), \Delta z_0 \in N\left(0, \sigma^2_{\Delta z}\right),$$

где $N\left(0, \sigma^2_{\Delta z}\right)$ – нормальный закон распределения величины $\Delta z_0 = z - z_0$, с нулевым математическим ожиданием и дисперсией $\sigma^2_{\Delta z}$ привязки к точному значению координаты z_0 фазового центра антенны НАП в системе координат WGS-84.

При этом уравнение состояния шкалы ККС в k -й момент передачи КИ, будет иметь вид

$$\Delta T_k = \Delta T_{k-1} + \left[1 - e^{-\alpha \Delta t}\right] \alpha^{-1} \frac{\Delta f_{k-1}}{f_0} + \xi_{\Delta T, k-1}, \quad (1)$$

где $\alpha \approx 0.1$ Гц – характеризует ширину энергетического спектра эталонного сигнала времени системы GPS, а $\Delta t = t_{k+1} - t_k$; $f_0 = 1.5 \cdot 10^9$ Гц – номинальное значение аналитической частоты сигнала L1 системы GPS; $\xi_{\Delta T, k-1}$ – гауссовский процесс типа белого шума с математическим ожиданием: $M\left[\xi_{\Delta f, k}\right] = 0$ и корреляционной функцией: $M\left[\xi_{\Delta f, k+1} \xi_{\Delta f, k}\right] = R_\xi \delta(\Delta t)$; Δf_{k-1} – частотные флуктуации сигнала системы GPS относительно эталонной частоты ККС.

Частотные флуктуации радионавигационного сигнала системы GPS задаются стационарным марковским процессом первого порядка с корреляционной функцией вида: $R_{\Delta f}(\Delta t) = \sigma^2_{\Delta f} e^{-\alpha |\Delta t|}$, где $\sigma^2_{\Delta f} \approx 0.25$ Гц^2 – мощность частотных флуктуаций сигнала системы GPS.

Корреляционные интегралы, формируемые в корреляторе НАП, позволяют отследить модуляцию сигнала НКА символами информации и вычислить метку времени во входном сигнале. Метки времени следуют с периодичностью 6 с для GPS. В пределах одного деления этой шкалы периоды дальномерного кода образуют 1 мс шкалу. Одна миллисекунда разделена в свою очередь на отдельные элементы для GPS – 1023 элемента. Потому в НАП относительное отклонение частоты опорного генератора представляется в виде разности метки времени, сформированной собственным генератором, и системной метки времени GPS, и выражается в мс. Получить относительное отклонение частоты опорного генератора НАП можно из соотношения

$$\Delta_{0 f_k} = \frac{\Delta f_k}{f_0} = -\frac{\Delta t_k / \tau_э}{1 + \Delta t_k / \tau_э},$$

где Δt_k – разность меток времени в мс, переданных НАП в k -й момент времени; а $\tau_э$ – длительность элементарного символа псевдослучайной последовательности дальномерного С/А-кода системы GPS ($\tau_э \approx 1$ мкс).

Намеренное искажение данных вектора состояния ККС является основной задачей кибератаки. Данный тип хакерской атаки относится к типу атак модификации [5]. Стандарты RTCM SC-104 определяют сообщения, которые содержат информацию о референцной станции (или ККС) и системные данные. Используя концепцию виртуальной референцной станций (Virtual Reference Station, VRS) [13] и внося ошибки в вычисления поправки в псевдодальности для каждой ККС, можно значительно исказить информацию потребителя о его истинном местоположении. Протокол NTRIP может быть использован для передачи RTCM данных для VRS. Корректирующая информация RTCM получается для виртуальной точки, соответствующей примерному местоположению пользователя, на основании данных с некоторого количества референцных станций (или ККС).

Таким образом, наиболее просто можно осуществить атаку на ККС путем создание VRS. Для этого необходимо осуществить следующую схему атаки:

1. Произвести идентификацию координатных, частотно-временных параметров ККС и осуществить их модификацию при передаче по сети Internet.

2. Произвести постановку помехи и блокировать ГНСС приемники ККС.

3. Осуществить эмуляцию «сырых» данных с блокированной ККС для не обнаружения модификации данных для пользователей локальной ККС при обработке их в центре сбора данных СДК.

Для осуществления успешной атаки необходимо знать метрологические характеристики аппаратуры: НАП и опорной квантовой меры частоты (КМЧ). При этом с учётом частотно-временных погрешностей, вносимых НАП, изменения относительного отклонения частоты $\Delta_{0 f_k}$ опорного генератора ККС должно определяться с погрешностью на суточном интервале наблюдения менее $1 \cdot 10^{-13}$. Кроме того, необходимо знать оценку погрешности расхождения шкал времени ККС относительно НКА и координированной шкалы UTC(UA). Пределы допускаемой погрешности измерения расхождения внутренней ШВ ККС относительно координированной шкалы UTC(UA) $\leq \pm$ 10 нс.

Предел допускаемой погрешности формирования дифференциальных поправок в формате RTCM SC-104, версия 2.2 (при доверительной вероятности 0,99) равен $\pm$ 0.3 м. Поэтому средняя квадратическая погрешность взаимной геодезической привязки координат (x, y, z) локальных (мобильных) ККС национальной СДК в системах геодезических параметров Земли ПЗ-90 или WGS–84 должна быть не более 0.1 м.

В настоящее время данные параметры (вектор состояния) получают на основании измерений с помощью дорогостоящих эталонных комплексов. Поэтому практическую апробацию атаки модификации вектора состояния ККС произведем на основе перехвата данных «сырых» измерений частотно-временных поправок кодовых наблюдений С/А кода на несущей частоте L1 навигационного сигнала GPS, принимаемого НАП. При этом атака модификации должна производиться в два этапа.

На первом этапе производится оценка суммарной погрешности навигационного сигнала GPS: погрешности, относящейся к НКА; погрешности, относящейся к НАП; погрешности, относящейся к среде распространения радиоволн [14]. Информация для первого этапа может быть получена из открытых источников и специализированных сайтов.

На втором этапе производится определение:

а) ковариационной матрицы результатов измерения ККС;

б) относительного отклонения частоты $\Delta_{0\,fk}$ опорной КМЧ из состава ККС;

в) оценки поправки $t = t_c + \Delta t_c$ к ШВ опорной КМЧ из состава ККС:

$$\Delta t_c = a_0 + a_1\left(t_c - t_{oc}\right) + a_2\left(t_c - t_{oc}\right)^2,$$

где a_0, a_1, a_2 – коэффициенты, передаваемые ККС в центр управления национальной СДК; t_c – время, передаваемое ККС; t_{oc} – опорное время блока временных данных, измеренное от начала еженедельной временной программы системы GPS.

Для второго этапа предлагается методика экспериментальной оценки вектора состояния ККС с помощью навигационного сигнала GPS, при использовании в качестве опорных генераторов рубидиевых КМЧ с оптической накачкой типа СЧВ–73, СЧВ–74. Выбор данного типа КМЧ обусловлен тем, что они широко используются в качестве высокостабильных источников сигналов для поверки опорных генераторов частотно-временной аппаратуры различных потребителей Украины, а также для хранения ШВ на образцах вооружения и военной техники. Кроме того, в методике учитывается, что в Украине широко распространена только одночастотная НАП, поэтому применяются алгоритмы, использующие только измерения С/А кода на несущей частоте L1 (1575,42 МГц) навигационного сигнала GPS.

В качестве НАП сигналов GPS/ГЛОНАСС предлагается использовать серийную аппаратуру национального производителя ГП „Оризон-Навигация" (г. Смела, серия СН). Например, устройство временной синхронизации с использованием сигналов GPS/ГЛОНАСС "Navior-S" (СН-3834) [15]. Данный НАП представляет собой 14-канальный специализированный приемник, работающий по сигналам спутников GPS/ГЛОНАСС, используя С/А и ПТ коды на несущей частоте L1. Сопряжение с ПЭВМ осуществляется по последовательным интерфейсам RS-232, с возможностью обмена информацией по протоколам NMEA 0183 (расширенный протокол), BINR (фирменный протокол «КБ НАВИС») и RTCM SC-104 v2.2 [10, 13, 16]. Кроме того, конструкция НАП типа СН-3834 позволяет в качестве опорного генератора использовать внешний генератор, что позволяет реализовать метод внешней синхронизации. Это необходимо для уменьшения влияния нестабильности частоты внутреннего опорного кварцевого генератора СН-3834 на результаты измерений ККС.

ЭКСПЕРИМЕНТАЛЬНАЯ ЧАСТЬ

Для осуществления кибератаки необходимо наряду с программными средствами применять и аппаратные средства. При этом минимально необходимые аппаратные средства, имитирующие работу стационарной ККС приведены на рис. 1. На схеме приемник СН-3834 синхронизируется сигналом опорной КМЧ частотой 5 МГц. Радионавигационные сигналы, принятые антенной, поступают на антенный вход СН-3834, с выхода которого сигнал "1PPS" (аппаратная метка времени) подается на вход "Б" частотомера типа Ч3-64/1. Секундная метка от опорного генератора СЧВ-74 подается на вход "А" частотомера Ч3-64/1. При этом частотомер работает в режиме измерения интервалов времени. Информация с выхода частотомера Ч3-64/1 через интерфейс IEEE488 передается в ПЭВМ для дальнейшей обработки и хранения. ПЭВМ оборудована платой контроллера интерфейса IEEE 488 (канала общего пользования ГОСТ 26.003-80), имеющую программную поддержку в стандарте VISA Revision 3.0.

Таким образом, с помощью частотомера Ч3-64/1 измеряется интервал времени, который соответствует размеру фазового сдвига между двумя этими сигналами, т.е. равняется времени задержки эталонного сигнала времени, который передается в составе навигационного сигнала, относительно системной ШВ ККС, формируемой СЧВ-74. Для хранения координированной шкалы UTC (UA) применяется синхронометр типа Ч7-37, который осуществляет привязку КИ в ККС и выдает в ПЭВМ через интерфейс IEEE488 информацию о коде текущего значения времени. Для усиления эталонных сигналов 5 МГц в ККС применяется усилитель высокочастотный распределительный типа ЯЗЧ–74.

При проведении эксперимента соблюдались нормальные климатические условия. Время наблюдения $\tau_н$ = 21970 с, интервал времени измерения $\tau_и$ = 1 с, темп выборки $\tau_в = \tau_и$. Информация о параметрах ШВ приемника была получена по COM-порту в протоколе BINR. Для работы с фирменным протоколом BINR на языке Borland C++Builder 6.0 было разработано специализированное программное обеспечение, позволяющее через интерфейс RS232 осуществлять доступ к «сырым» измерениям частотно-временных поправок кодовых наблюдений С/А. Для этого в НАП посылался запросный пакет 1f. Ответный пакет №72 протокола BINR содержит информацию о времени. При этом учитывалось, что пакет №72 передается с опережением на 300–400 мс относительно выходного импульса 1PPS. Данные, выдаваемые ответным пакетом №72 (данные о частоте и времени) протокола обмена BINR: текущее относительное отклонение частоты опорного генератора с точностью $1 \cdot 10^{-10}$ и текущее отклонение меток времени от шкалы UTC (нс).

Необходимо также получать данные, выдаваемые ответным пакетом №84 (последнее решение) протокола обмена BINR: широта (радианы), долгота (радианы), высота (метры), время определения (мс), среднее квадратичное отклонение (СКО) координат (метры).

Задержка сигнала в тракте от антенны до измерителя временного интервала в НАП компенсируется за счет соответствующей калибровки приемника.

При помощи программного обеспечения «сырые» данные НАП СН-3834 преобразовываются в КИ и в формате RTCM SC-104 посылаются на сервер NTRIP. В задачу сервера входило распространение КИ посредством сети Internet. В ходе эксперимента вырабатывалась и доставлялась потребителю КИ, содержащая поправки только к кодовым измерениям (кадры RTCM SC-104 № 1, 31).

Данные о сдвиге шкалы ΔT, переданные в составе частотно-временного пакета № 72 протокола BINR и обрабатываемые с помощью разработанного программного обеспечения, приведены на рис. 2.

Из анализа данных следует, что если абсолютное значение разности между измеренной в приемнике и расчетной ШВ превышает порог 12 нс, то приемник делает сдвиг своей ШВ на 12 нс соответственно вперед или назад во времени. Некомпенсированный остаток от разности указанных ШВ округляется до одной наносекунды и передается в составе частотно-часового пакета № 72 протокола BINR. Отсюда следует, что погрешность измерения значения кода фазы (code phase) соответственно равна $\tau_э / N_{кв} \approx 0.98$ нс, где $N_{кв} = 2^{10}$ – число, определяемое схемой слежения СН-3834 за задержкой огибающей сигнала.

При этом погрешность формирования сигнала на выходе 1PPS в режиме слежения за НКА становится не более 25 нс. Таким образом, обеспечивается стабильность воспроизведения приемником СН-3834 меток времени UTC с погрешностью ± 12 нс.

Выделяя в данной последовательности чисел 12 нс скачки фазы и компенсируя их получим последовательность, представленную на рис. 3. Применяя метод наименьших квадратов, определим в данной последовательности линейную функцию ухода ШВ опорной КМЧ вида

$$T(t_k) = \Delta_{0 f_k} t_k + T_0, \qquad (2)$$

где T_0 – разность шкалы КМЧ и системной шкалы GPS, соответствующая начальному моменту времени t_0.

При этом гистограмма и плотность вероятности невязок ШВ относительно $T(t_k)$ будет иметь вид, представленный на рис. 4.

Для описания статистической модели невязок значений ШВ было взято семейство распределений с плотностью вероятности вида:

$$f(\Delta T_k, m_i, \sigma_i, \kappa_i, I) = \sum_{i=1}^{I} \left[\frac{\kappa_i}{\sigma_i \sqrt{2\pi}} \exp\left(\frac{\Delta T_k - m_i}{2\sigma_i^2} \right) \right],$$

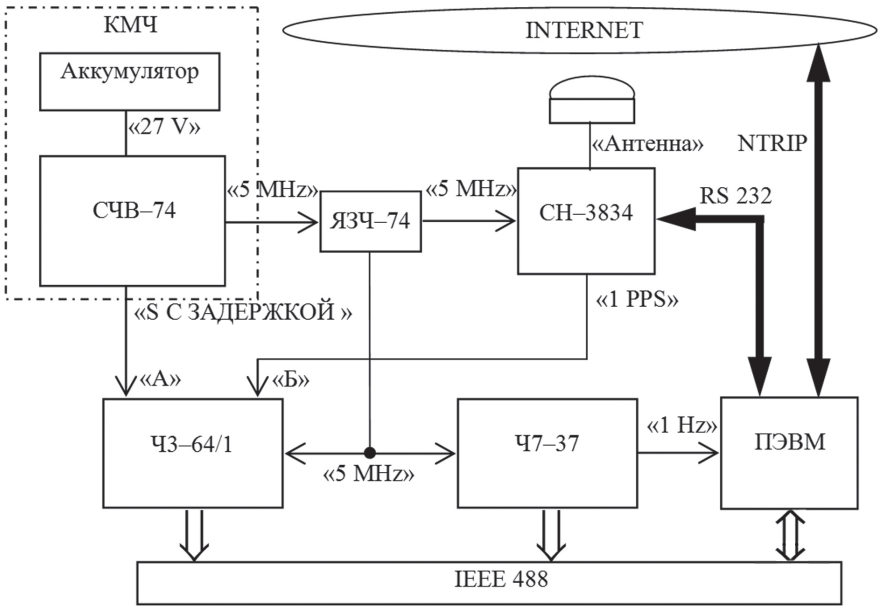

Рис. 1. Функциональная схема стационарной ККС с опорной КМЧ типа СЧВ-74

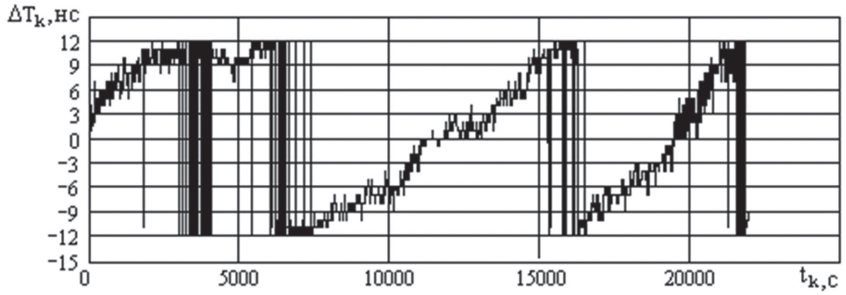

Рис. 2. График «сырых» данных результатов сличения поправок ШВ, переданных в составе частотно-временного пакета № 72 протокола BINR

где $m_i, \sigma_i^2, \kappa_i$ – математическое ожидание, дисперсия, нормировочный коэффициент *i*-й плотности нормального распределения, а параметр $I = 3$.

Поиск неизвестных параметров $m_i, \sigma_i^2, \kappa_i$ данного распределения проводился методом наименьших квадратов [17]. Проверка гипотезы о законе распределения проводилась с использованием критерия согласия «хи-квадрат».

Найденные плотности распределения невязок значений ШВ для ККС изображены на рис. 4 штрих пунктиром.

В данном случае относительного отклонения частоты опорного генератора $\Delta_{0fk} = 2.5 \cdot 10^{-12}$. При этом СКО значений $\Delta\tau$ от линейной функции составляет 4.2 нс.

Доверительный интервал определения относительного отклонения действительного значения частоты от своего номинального значения на суточном интервале наблюдения при таком значении СКО составляет $1.5 \cdot 10^{-13}$. Таким образом, использование уточняющей частотно-временной информации, переданной в составе пакета № 72 протокола BINR приемника СН-3834, позволяет, с одной стороны, уменьшить значение доверительного интервала определения действительного значения частоты КМЧ, а, с другой стороны, остается недостаточным для определения метрологических характеристик прецизионных КМЧ из состава ККС. Это приводит к необходимости поиска алгоритмов дополнительной компенсации флуктуаций меток времени, переданных НАП типа СН-3834, с целью их использования для оценки относительного отклонения действительного значения частоты Δ_{0f} опорного генератора ККС с погрешностью на суточном интервале наблюдения $\leq 1 \cdot 10^{-13}$.

Приемник СН-3834 выделяет метки времени, переданные каждым НКА из числа рабочего созвездия, и измеряет интервалы времени между меткой времени своей собственной ШВ, сформированной внутренним опорным генератором (при внешней синхронизации – КМЧ, подключенным на вход внешней синхронизации) и метками времени, принятыми от каждого НКА. Данные интервалы времени используются как исходная информация для навигационной задачи определения координат ККС на основе разностно-дальномерного метода. Знание координат ККС разрешает определить дальность до каждого НКА из состава рабочего созвездия. Используя значение скорости распространения радиоволны, эти дальности могут быть пересчитаны в абсолютные значения задержек ШВ каждого НКА, обусловленных временем распространения сигнала от НАК до НАП. Поэтому погрешности определения координат ККС будут непосредственно входить в состав погрешности синхронизации шкалы ККС.

Определение интервала времени задержки системной ШВ в приемнике СН-3834 осуществляется путем расчета времени распространения от НКА, который находится в зените, относительно места положения фазового центра антенны. В этом случае влияние ионосферы на скорость распространения электромагнитной волны будет минимальным. Поэтому основной вклад в погрешность определения задержки будет вносить погрешность определения места положения фазового центра антенны приемника по высоте.

На рис. 5 приведены результаты определения места положения по высоте с помощью приемника типа СН-3834 для стационарной ККС, которые передаются в составе пакета № 84.

Если сравнить данные результатов определения местоположения ККС по высоте с резуль-

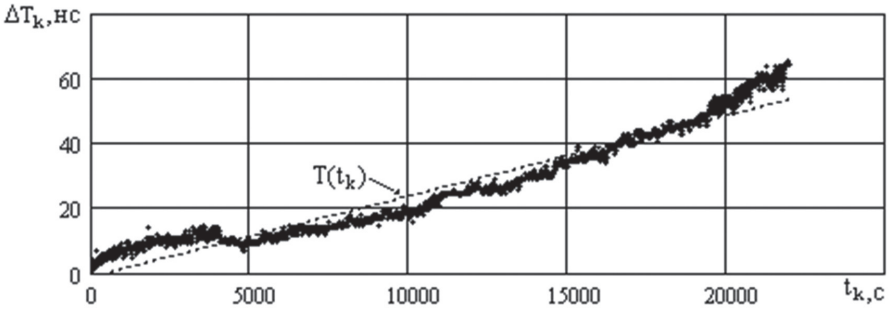

Рис. 3. График ухода ШВ после устранения неоднозначности значения кода фазы на несущей частоте

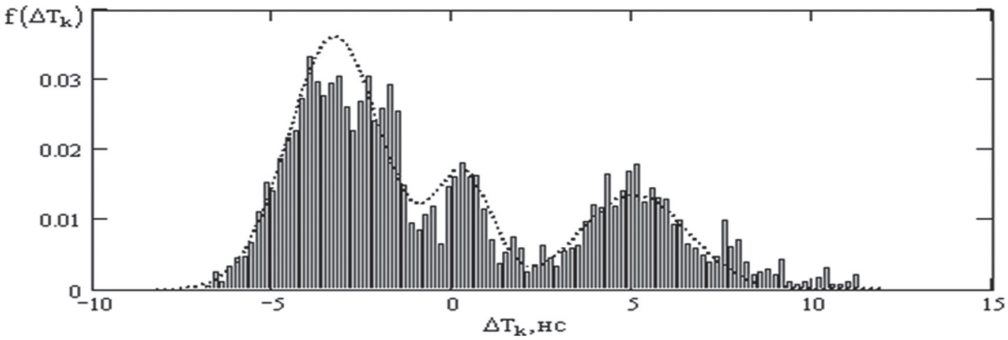

Рис. 4. Гистограмма и плотность вероятности измерений невязок ШВ

татами отклонений аппаратной метки времени приемника от аппроксимации линейной функцией (приведенной на рис. 3), можно увидеть их качественное совпадение. Результаты сравнения приведены на рис. 6.

Количественной мерой степени связи двух случайных процессов есть коэффициент их взаимной корреляции, который рассчитывается по формуле

$$R_{h,\Delta\tau} = \frac{\frac{1}{N}\sum_{k=1}^{N}\left[h_k - M(h_k)\right]\left[\Delta\tau_k - M(\Delta\tau_k)\right]}{\sqrt{D(h_k)D(\Delta\tau_k)}}, \quad (3)$$

где $N = \tau_н/\tau_в$ – количество наблюдений (объем выборки); $M(h_k) = \frac{1}{N}\sum_{k=1}^{N} h_k$ – оценка математического ожидания высоты потребителя над геоидом, полученная по результатам выборки последнего решения, представленного в пакете № 84 протокола BINR приемника СН-3834; $M(\Delta\tau_k) = \frac{1}{N}\sum_{k=1}^{N}\Delta\tau_k$ – оценка математического ожидания отклонения поправок к аппаратным меткам времени, сформированных в пакете № 72 протокола BINR приемника СН-3834, от линейной функции вида (2); $D(h_k) = \frac{1}{N}\sum_{k=1}^{N}\left[h_k - M(h_k)\right]^2$ – оценка дисперсии определения места положения над уровнем моря потребителя, полученная по результатам выборки последнего решения, представленного в пакете № 84 протокола BINR приемника СН-3834; $D(\Delta\tau_k) = \frac{1}{N}\sum_{k=1}^{N}\left[\Delta\tau_k - M(\Delta\tau_k)\right]^2$ – оценка дисперсии поправок к аппаратным меткам времени, сформированных в пакете № 72 протокола BINR приемника СН-3834, от линейной функции (2).

Для данной реализации значение $R_{h,\Delta\tau}$ равняется 0.8, что свидетельствует о наличии сильной связи между двумя случайными процессами. Это позволяет использовать информацию об отклонении определения места положения ККС по высоте от своего среднего значения с целью компенсации погрешности определения отклонения аппаратной ШВ приемника СН-3834 от координированной шкалы UTC (USNO).

С этой целью введем поправку к метке времени, сформированной в k-й момент времени

$$\delta\tau_k = m_t \Delta h_k, \quad (4)$$

где Δh_k – отклонение оценки места положения ККС по высоте от своего среднего значения, полученное в k-й момент времени; m_t – некоторый коэффициент пропорциональности, который разрешает согласовать размерности величин, которые входят в выражение (4) и оптимизировать вес данной поправки.

С учетом выражения (4), уточненное значение поправки ΔT, переданное в составе пакета № 72 протокола BINR приемника СН-3834, можно определить с помощью следующего соотношения

$$\Delta T_{y,k} = \Delta T_k - \delta\tau_k, \quad (5)$$

где ΔT_k – значение поправки к аппаратной ШВ приемника, переданное в составе пакета № 72 протокола BINR.

Коэффициент m_t, который входит в состав выражения (4), существенным образом влияет на количественное значение оценки погрешности задержки ШВ, обусловленной погрешностью определения места положения ККС. Поэтому естественной является его оптимизация.

Оптимизацию коэффициента m_t целесообразно проводить на основе минимизации отклонения поправки $\Delta T_{y,k}$ от ее аппроксимации

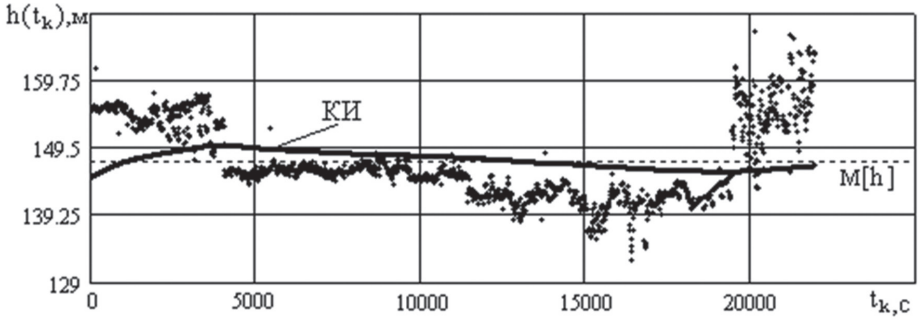

Рис. 5. Результаты определения местоположения ККС по высоте с помощью НАП типа СН-3834

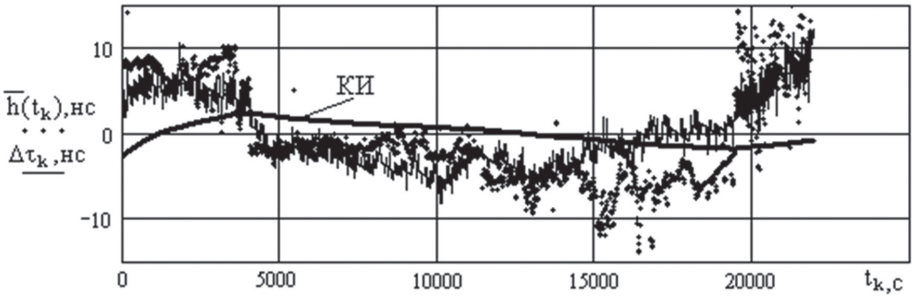

Рис. 6. Результаты сравнения определения местоположения ККС и отклонений аппаратной метки времени приемника от аппроксимации линейной функцией

линейной функцией вида (2), что представляет собой условное среднее значение отклонения аппаратной ШВ от шкалы UTC (USNO). Количественной оценкой отклонения случайного процесса от условного среднего есть его дисперсия вида

$$\sigma^2_{\Delta\tau} = \frac{1}{N}\sum_{k=1}^{N}\left[\Delta T_{y,k} - T(t_k)\right]^2 . \qquad (6)$$

Зависимость СКО от величины коэффициента m_t приведена на рис. 7. Видно наличие явного минимума СКО в окрестности значения m_t=0.56. При этом само значение СКО уменьшается от значения $17.2 \cdot 10^{-9}$ до значения $6.7 \cdot 10^{-9}$. Дальнейшее уменьшение значения среднего квадратичного отклонения $\sigma_{\Delta\tau}$ возможно путем применения цифрового рекурсивного фильтра [4]. Применим рекурсивный фильтр следующего вида

$$\Delta\bar{T}_k = (1-\alpha)\Delta\bar{T}_{k-1} + \alpha\left[\Delta T_{y,k} - T(t_k)\right] . \qquad (7)$$

Решение задачи синтеза рекурсивных фильтров сводится к нахождению коэффициента α. Известны прямые и косвенные методы синтеза рекурсивных фильтров [3, 17]. Прямые методы основаны на непосредственном определении параметров цифровых рекурсивных фильтров по заданным временным или частотным характеристикам. Косвенные методы синтеза рекурсивных фильтров основаны на дискретизации аналогового фильтра, удовлетворяющего заданным требованиям. Применяя косвенный метод синтеза рекурсивного фильтра, получим значение коэффициента α=0.1. Данный коэффициент позволяет фильтру устранить имеющиеся большие одиночные выбросы и существенным образом сгладить флуктуации поправки к аппаратной ШВ и соответственно уменьшить значение СКО и, в то же время, оставаться чувствительным к медленным вариациям поправки, обусловленным изменением частоты внешней синхронизирующей КМЧ.

Результат сглаживания приведен на рис. 8 штриховой линией. Сплошной линией приведены исходные результаты отклонения поправки к аппаратной ШВ от линейной аппроксимирующей функции вида (2).

СКО результирующей поправки от линейной аппроксимирующей функции составляет $2 \cdot 10^{-9}$ с, что позволяет уменьшить доверительный интервал определения относительного отклонения частоты на суточном интервале наблюдения до значения $6 \cdot 10^{-14}$. Такое значение доверительного интервала уже есть приемлемым для получения достоверных оценок относительного отклонения действительного значения частоты КМЧ с необходимой точностью на основе анализа «сырых» данных, что эквивалентно сличению с более стабильными мерами частоты: водородными или цезиевыми КМЧ.

Таким образом, использование в обработке данных протокола №72 позволяет на порядок повысить точность определения относительного отклонения действительного значения частоты на суточном интервале наблюдения в сравнении с использованием аппаратной метки (с $2 \cdot 10^{-12}$ до $2 \cdot 10^{-13}$). При этом предлагаемый алгоритм компенсации погрешности формирования метки времени повышает точность определения оценки относительного отклонения действительного значения частоты опорного генератора вдвое, т.е. до $6 \cdot 10^{-14}$.

Оценка трёх координат в векторе состояния ККС в системе WGS-84 по данным выдаваемым пакетом №84 (последнее решение) протокола обмена BINR приемника СН-3834 имеет вид: x=3322269.4975 м; y=2428959.4668 м; z = 4901486.0223 м. Математическое ожидание $M[h]$ высоты фазового центра антенны НАП в системе WGS-84 равно 147.67 м. Сравним данную оценку высоты с эталонной, которая вычислена на основании данных стереотопографической съемки, полученной от Харьковского городского управления архитектуры. Так, значение нормальной высоты h_γ фазового центра приемной антенны (ПКАН.434854.023) в местной системе координат равно 151.93 м. Однако высота h_{WGS-84} представляет собой геодезическую высоту: высоту точки земной поверхности над рассматриваемым эллипсоидом, отсчитанную по нормали к его поверхности. При этом высоты, полученные по материалам нивелирования земной поверхности и приводимые в геодезических каталогах и на топографических картах, относятся к системе нормальных высот, которая применяется в нашей стране. С учетом того, что нормальные высоты в Украине отсчитываются от поверхности квазигеоида Земли в Балтийской системе высот 1977 года, то геодезическая высота h_{WGS-84} определятся в виде

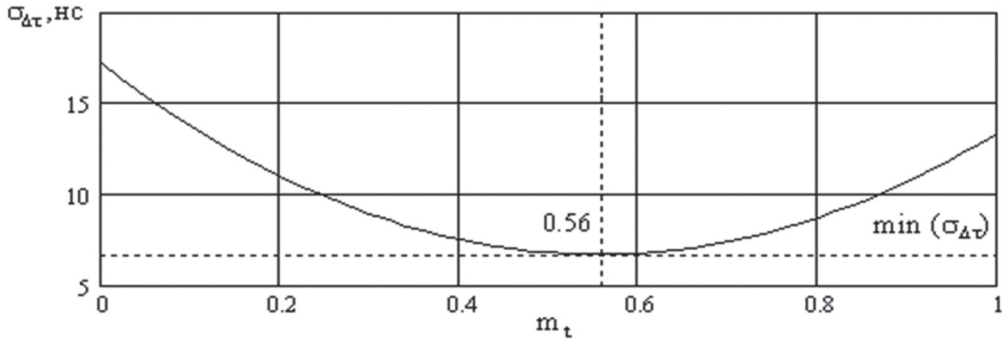

Рис. 7. Зависимость СКО ШВ от величины коэффициента m_t

$$h_{WGS-84} = h_\gamma + \Delta h + \zeta,$$

где Δh – разность высот, которую можно определить через матричные преобразования системы ПЗ-90 в систему WGS–84 [2,3], ζ – аномалия высоты (превышение квазигеоида над эллипсоидом ПЗ-90). При этом погрешность от аномалии высоты для системы WGS–84 может лежать от 2 до 6 м [8]. Величина ζ связана с аномалией гравитационного поля и меняется в зависимости от координат и составляющих уклонений отвесной линии. В целом значения ζ для разных территорий Украины определены. Однако для общего земного эллипсоида ПЗ–90 и референц-эллипсоида Красовского они не совпадают.

Таким образом, используя два протокола из состава внутреннего программного обеспечения НАП типа СН-3834 возможно без применения эталонного оборудования оценить вектор состояния ККС с высокой точностью.

Модификация данных вектора состояний ККС при таком виде атаки позволит полностью захватить управление выдачи КИ в СДК. Для устранения данной угрозы необходимо применять процедуру аутентификации КИ в ККС, которая представляет собой процедуру проверки того, что полученные данные пришли от указанной ККС и не были модифицированы. При этом аутентификация КИ должна также предполагать проверку порядка следования и своевременность доставки сообщений.

Техника аутентификации данных в ККС предполагает присоединение к КИ созданного с использованием секретного ключа небольшого блока данных фиксированного размера, называемого криптографической контрольной суммой или кодом аутентификации сообщения (Message Authentication Code, MAC). При этом предполагается, что две участвующие в обмене данными стороны, ККС и потребитель, используют общий секретный ключ К. Чтобы послать сообщение М (КИ) потребителю В, отправитель (ККС) вычисляет код аутентификации сообщения как функцию сообщения и ключа:

$$\mathrm{MAC} = C_K(M),$$

где М – сообщение переменной длины; К – секретный ключ, известный только отправителю (ККС) и получателю (потребителю); $C_K(M)$ – аутентификатор фиксированной длины.

Сообщение с добавленным к нему значением МАС пересылается потребителю КИ. Потребитель КИ выполняет аналогичные вычисления с полученным сообщением (КИ), используя тот же секретный ключ, чтобы вычислить новое значение МАС. Вычисленное значение МАС сравнивается с полученным вместе с сообщением (КИ) значением.

Для КИ, передаваемой национальной СДК, предлагается применять функцию вычисления значения МАС, называемую алгоритмом аутентификации данных (Data Authentication Algorithm), который основан на использовании DES [9].

ВЫВОДЫ

1. Киберугрозы представляют собой основной вызов для будущего применения ГНСС. Кибератаки могут воздействовать как на бортовые, так и на наземные системы, а методы воздействия могут простираться от простых асимметричных атак, типа глушения, до высокосложных электронных систем и программных атак.

2. С целью устранения атаки модификации на сервер ККС информация (внутренняя информация) о высоте фазового центра антенны НАП и параметрах опорного генератора обязательно должна шифроваться.

3. В качестве примера с помощью имитационного комплекса было проведено моделирование работы ККС в реальном времени. Показано, что применение МАС кода делает не возможной атаку на основе применения концепции VRS.

4. Самая простая кибератака на СДК основана на невозможности реализации надежного определения подлинности КИ в условиях применения «одностороннего» канала связи. Так как в этой ситуации хорошо срабатывает известная хакерская атака повторением сигнала (replay attack). Поэтому для контроля достоверности КИ обязательно требуется дублирующий радиоканал передачи данных, который достаточно сложно подавить средствами радиоэлектронной борьбы.

Литература

[1] Українська мережа станцій космічної геодезії та геодинаміки (Укргеокосмомережа) / [О.В. Болотіна, С.Л. Болотін, М.М. Медведський та ін.] ; за ред. Я. С. Яцківа. — К.: ВАІТЕ, 2005. – 62 с.

[2] Одуан К. Измерение времени. Основы GPS / Одуан К., Гино Б. ; пер. с англ. – Москва: Техносфера, 2002. – 400 с.

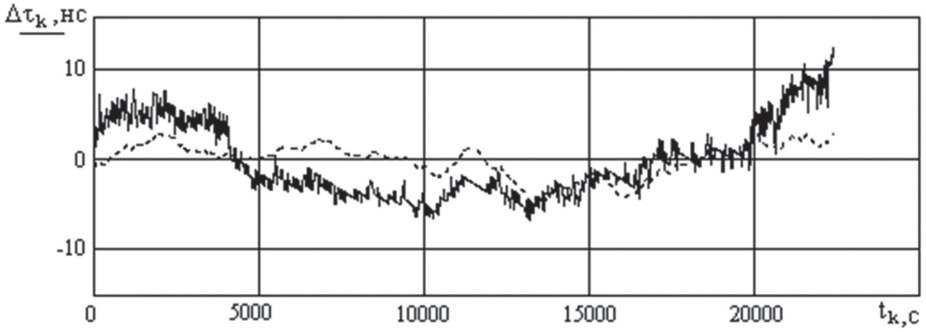

Рис. 8. Результат сглаживания с помощью цифрового рекурсивного фильтра

[3] ГЛОНАСС. Принципы построения и функционирования / [Бакитько Р.В., Болденков Е.Н., Булавский Н.Т. и др.] ; под ред. А.И. Перова, В.Н. Харисова. Изд. 4-е, перераб. и доп. – М: Радиотехника, 2010. – 800 с.

[4] Глобальные навигационные спутниковые системы. Системы дифференциальной коррекции. Общие технические требования : ГОСТ Р 54459–2011 – [Дата введения – 2012–07–01]. – М. : Стандартинформ, 2012. – 18 с. (Национальный стандарт Российской Федерации).

[5] Tyler Nighswander, Brent Ledvina, Jonathan Diamond, Robert Brumley, David Brumley. GPS Software Attacks. Proceedings of the ACM Conference on Computer and Communications Security (CCS), October 16–18, 2012, Raleigh, North Carolina, USA. (Nov28_ GPS.pdf)

6] Nils Ole Tippenhauer, Christina Pцpper, Kasper Bonne Rasmussen, and Srdjan Capkun. On the requirements for successful GPS spoofing attacks. Proceedings of the ACM Conference on Computer and Communications Security (CCS), 22:75–85, 2011.

[7] Mark L. Psiaki, Brady W. O'Hanlon, Jahshan A. Bhatti, Daniel P. Shepard, and Todd E. Humphreys. Civilian GPS Spoofing Detection based on Dual-Receiver Correlation of Military Signals. In Proceedings of the Institute of Navigation GNSS (ION GNSS 2011), September 2011.

[8] Глобальная навигационная спутниковая система. Форматы передачи корректирующей информации. Технические требования : ГОСТ Р 53610-2009 – [Дата введения – 2011–01–01]. – М. : Стандартинформ, 2011. – 20 с. (Национальный стандарт Российской Федерации).

[9] Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : монографія. – Харків: Видавництво «Форт», 2010. – 608 с.

[10] Radio Technical Commission for Maritime Services Recommended Standards for Differential GNSS Service (RTCM SC-104) Version 2.2, 1998.

[11] Система спутниковая навигационная глобальная. Термины и определения : ГОСТ Р 52928-2008 – [Дата введения – 2008–07–20]. – М. : Стандартинформ, 2008. – 11 с. (Национальный стандарт Российской Федерации).

[12] Глобальная навигационная спутниковая система. Станция контрольно-корректирующая локальная гражданского назначения. Технические требования : ГОСТ Р 52866–2007 – [Дата введения – 2008–07–01]. – М. : Стандартинформ, 2008. – 7 с. (Национальный стандарт Российской Федерации).

[13] National Marine Electronics Association (NMEA 0183) Standard for Interfacing Marine Electronic Devices (Version 2.30), 1998.

[14] Interface Control Document: NAVSTAR GPS Space Segment/ Navigation User Interfaces (ICD-GPS-200). – Rockwell Int. Corp., 1997.

[15] Устройство временной синхронизации с использованием сигналов GPS/ГЛОНАСС "NAVIOR-S" СН-3834. Руководство эксплуатации ТДЦК.461513.030 РЭ. – 2000. – 38 с.

[16] Аппаратура потребителей спутниковых навигационных систем ГЛОНАСС и NAVSTAR. Протокол обмена BINR. ПКАН.461513.015 Д2. – 2000. – 35 с.

[17] Чирков А.Г., Матисов Б.Г. Современная теория стабильности прецизионных генераторов. СПб. Издательство Политехнического университета, 2005. – 355 с.

Поступила в редколлегию 29.04.2013

Гриненко Татьяна Алексеевна, канд. тех. наук, ст. преподаватель кафедры БИТ ХНУРЭ. Научные интересы: методы и средства криптографической защиты информации.

Нарежний Алексей Павлович, старший научный сотрудник отдела, Метрологический центр военных эталонов Вооруженных Сил Украины. Научные интересы: частотно-временные измерения и системы единого времени.

УДК 621.317.76.089.68:621.373.82

Застосування кодів автентифікації повідомлень для виявлення модифікацій даних у регіональних системах диференціальної корекції навігаційних сигналів систем GPS/ГЛОНАСС / Т.О. Гріненко, О.П. Нарєжній // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 301–310.

У статті обґрунтовується необхідність застосування кодів автентифікації повідомлень (MAC) для забезпечення цілісності і достовірності коригуючої інформації, що формується системами диференціальної корекції навігаційних сигналів систем GPS/ГЛОНАСС. На прикладі роботи типової схеми контрольно-коригуючої станції обґрунтовується необхідність застосування MAC-алгоритмів при передачі "сирих" вимірів уточнених ефемерид і частотно-часових поправок навігаційно-космічних апаратів глобальних навігаційних супутникових систем GPS/ГЛОНАСС.

Ключові слова: контрольно-коригуюча станція, захист даних, криптографія, коди автентифікації повідомлень.

Іл.: 08. Бібліогр.: 17 найм.

UDC 621.317.76.089.68:621.373.82

Message authentication codes application for data modification detection in regional systems of differential correction of GPS/GLONASS systems navigation signals / T.O. Grinenko, O.P. Narezhniy // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 301–310.

The paper substantiates the need of message application codes (MAC) application for ensuring integrity and validity of correction information formed by differential correction systems of GPS/GLONASS systems navigation signals. The need of MAC-algorithms application during transmission of raw measurement data of specified ephemeris and frequency and time corrections of space navigation vehicles of GPS/GLONASS global navigation satellite systems is substantiated using an example of the operation of a control-correction station typical scheme.

Keywords: control correction station, data protection, cryptography, message authentication codes.

Fig.: 08. Ref.: 17 items.