АЛГОРИТМ ВИЯВЛЕННЯ ВПЛИВУ СПУФІНГУ ПІД ЧАС ВИКОНАВЧОЇ ПРОКЛАДКИ ПРОГРАМНИМИ ЗАСОБАМИ ЕЛЕКТРОННОЇ КАРТОГРАФІЧНОЇ НАВІГАЦІЙНО-ІНФОРМАЦІЙНОЇ СИСТЕМИ

УДК 656.61

DOI: https://doi.org/10.35546/2313-0687.2019.25.30-38

Петровський Андрій Валерійович
кандидат технічних наук, доцент, доцент кафедри судноводіння та електронних навігаційних систем
Херсонської державної морської академії, м. Херсон, Україна, **E-mail:** andreyanybody@gmai.com, ORCID ID: *0000-0002-3337-9577*

Анотація. Метою статті є розробка алгоритму виявлення впливу спуфінгу під час виконавчої прокладки. Пропонується розробити алгоритм виявлення спуфінгу засобами електронної картографічної навігаційно-інформаційної системи із можливостями усунення його наслідків. Після імплементування програмної реалізації алгоритму soft-девелоперами, передбачається оновлення програмного забезпечення бортової електронної картографічної навігаційно-інформаційної системи при заході в порт, де є їх представники. У процесі дослідження використані методи дослідження: емпіричні (порівняння) та теоретичні (аналіз та синтез) з використанням теорії навігації, інформаційних систем та алгоритмів, особливостей електронних картографічних систем.

Основні результати дослідження. Розроблений алгоритм засновано на аналізі треку позицій судна. Всі позиції треку на цей час бортовою електронною картографічною навігаційно-інформаційною системою встановлюються на електронну карту при виборі оператором відповідного режиму, але не відслідковуються та не аналізуються. На основі отриманих географічних координат позицій формується тренд, який оцінює можливість роботи пристрою під контролем при порівнянні тренду і даних з іншого джерела позиціонування, якщо воно є, наприклад з Echo reference або Estimated position, з даними приладів GPS|DGPS. Якщо сталося значне відхилення, алгоритм розраховує маршрут повернення на найближче плече маршруту з використанням відповідних інструментів електронної картографічної навігаційно-інформаційної системи. У разі їх відсутності – надається рекомендований перелік географічних координат для ручної побудови маршруту повернення.

Наукова новизна. Оскільки останні дослідження та вирішення поставлених питань протидії спуфінгу здійснювалися у розрізі встановлення додаткового обладнання та визнання необхідності наявності у штурмана більш поширених знань з області теорії радіосигналів, наданий алгоритм полегшить визначення моментів зовнішнього контролю суднового обладнання GPS|DGPS програмними засобами та стане основою для подальших досліджень з вирішення цієї проблеми для комерційного та пасажирського транспорту. Практична значимість досягається у кількох

напрямках: немає необхідності у додатковій освіти штурманів з теорії радіосигналів – достатньо стандартної підготовки; є можливість визначати момент часу захвату контролю; здійснюється автоматизована побудова в інтерактивному режимі маршруту повернення на обране плече маршруту, у разі значного відхилення істинної позиції судна за даними проведеної обсервації / іншого джерела позиціонування та аналізу треку від позиції за даними GPS|DGPS; поповнення бази даних відповідних організацій для випуску Admiralty Information Overlay з метою покращення уваги штурманів у даному районі.

Ключові слова: *електронна картографічна навігаційно-інформаційна система, спуфінг, алгоритм, GPS.*

Постановка проблеми. Використання електронної картографічної навігаційно-інформаційної системи (ЕКНІС) для потреб судноплавства давно э нормою, але з полегшенням праці штурмана та подальшим розвитком прогресу в цієї області, завдяки автоматизації більшості функцій навігації, виникають також негативні керовані явища, які надають недовіри до таких систем. У останні роки все більш з'являється інформації щодо використання технологій впливу на коректність роботи програмного забезпечення керуванням судна. Наприклад, при використанні e-mail можлива підміна адресу відправника, і, відповідно, заміна вкладених файлів [1,2]. Незважаючи на те, що фальсифікація карт S-63 доволі утруднена завдяки шифруванням та іншим механізмам захисту, отримання оновлень через e-mail не є повністю безпечним, особливо при недбайливому відношенні щодо безпеки використання USB портів встановленого обладнання. Розроблені засоби захисту [3] потребують додаткових знань від операторів спеціалізованого програмного забезпечення, тому у подальшому не розглядаються. Поряд з цим поширюється використання спуфінгу. Цю технологію використовують для поширення шкідливого програмного забезпечення, викрадення даних, а також з метою обходу механізмів контролю доступу.

Помилкові сигнали дають можливість змінити курс судна і направити його в територіальні води іншої країни, причому як з метою створення напруги на міжнародній арені [4], так і з метою піратства [5], захоплення вантажу або екіпажу. Спотворення сигналів GPS є не тільки російською практикою [6], ці методи використовують і інші країни, з метою дезорієнтації навігації поблизу стратегічно важливих об'єктів [7]. У звіті [8], який було опубліковано у 2019р. надано статистику за 2017-2018рр., де вказано кількість випадків спуфінгу для більш ніж 1300 судів. На даний час з'ясовані акваторії, де використовуються найбільш часто спуфінг: Чорне море [9], Фінська затока [10], Владивосток, Сірія [8] та побудовано карту статистики використання такої технології у акваторії Чорного моря (рис. 1).

Військові суда мають більш потужний сигнал, тому здійснити такого роду атаку дуже складно, але громадянські суда – інша справа. Спуфери пригнічують відносно слабкі сигнали GNSS за допомогою радіосигналів, що несуть неправдиву інформацію про місцезнаходження. Велика кількість цивільних пристроїв GPS робить громадянське шифрування непрактичним, а також це йде проти оригінальної мети творців GPS, яка повинна була забезпечити вільний доступ до GPS кожному і всюди. Відомості, що GPS піддається атакам, змушує багато країн шукати йому альтернативу: eLoran, eChayka [11]. За словами фахівців в області кібербезпеки, основна проблема GPS- і GNSS (Global Navigation Satellite Systems) систем полягає в слабких сигналах, які передаються на висоті близько 20 тис. кілометрів над Землею і можуть глушитися хакерами за допомогою дешевих і доступних «глушилок». З іншого боку, сигнали eLoran заглушити складніше, так як в середньому вони в 1,3 млн разів сильніше в порівнянні з сигналами GPS. Розвиток таких напрямків – додаткове навантаження на бюджет країн, тому на даний момент актуальність розробки методів та засобів боротьби із спуфінгом не підлягає сумніву.

Існує два способи спуфінгу:

- ретрансляція сигналів GNSS, записаних в іншому місці або часу (так званий meaconing – введення похибки навмисними перешкодами);
- генерація і передача модифікованих супутникових сигналів.

Головним компонентом пристрою-спуферу є імітатор GPS-сигналів. Сучасні технології з року в рік зменшують собівартість виробництва компонентів інтегральних схем, і тому, такі пристрої є у вільному продажі вартістю від 1000$. Однак, внаслідок особливостей функціонуван-

ня такі імітатори мають радіус дії до 10 м, при використанні підсилювачів – хибний сигнал GPS збільшується в десятки разів. Ідеальним моментом для підміни сигналів з кодом стандартної точності є моменти, коли зв'язок із справжніми супутниками пропадає або дуже слабкий [12]. Перш за все така технологія передбачає запуск процесу дублювання реальних сигналів зі супутників, з метою повної відповідності по характеристикам. Далі, збільшують потужність хибних сигналів. При цьому навігаційна система вважає їх головними та фільтрує реальні сигнали як перешкоди. Контроль над СНС встановлено [13]. Можливі варіанти подальшого розвитку подій: поступово змінювати відомості місцезнаходження для плавної зміни курсу судна з метою приводу судна у визначену акваторію [14] або повністю дезорієнтувати оператора навігаційної системи.

Рис. 1 – Карта випадків спуфінгу [8]

Об'єктом дослідження статті є результати впливу на ЕКНІС використання спуфінгу у морі/прибережних водах. Предмет дослідження **–** наукові та практичні рішення з виявлення та боротьби із спуфінгом.

Аналіз останніх досліджень і публікацій. У 2001 Міністерство транспорту США розробило міри для протидії спуфінгу, які базувалися на використанні додаткових апаратних пристроїв та збереження робочих місць замість комп'ютеризації, що є досить дорогим рішенням. У подальшому для 5 із 6 контрмір дослідниками Корнелльського університету та технологічного університету Вірджинії було подолано.

Марк Псіакі запропонував схему захисту від GPS-спуфинга Його група створила модифікований GPS-приймач з антеною, яка змінює своє положення з певною частотою. Оскільки супутники знаходяться на значній відстані один від одного, а помилкові сигнали приходять з одного близького місця (прибережної зони), фаза несучого коливання в для такого приймача буде змінюватися по-різному, що і дозволить розпізнати обман [15].

Пристрій від Mitre -Time Anomaly Detection Appliqué (TADA) захищає сучасні цифрові системи від спуфінг-атак. Система безперервно порівнює вивірені параметри: відому частоту або місцезнаходження, з тими, що надає GPS-приймач. Коли з'являється різниця між даними, TADA видає тривогу. Недолік: різниця, якщо її робити дуже плавно, може не перевищувати параметрів безпеки щодо відхилення від курсу [16].

Передові технології придушення перешкод, такі як AIM +, використовують алгоритми обробки сигналів для реєстрації шляхів виявлення різних аномалій в сигналі. З реалістичними рівнями потужності та фактичними навігаційними даними в сигналі AIM + може ідентифікувати «неаутентичний» сигнал. Також використання антени подвійний поляризації сприяє зменшенню ймовірності впливу спуфінгу.

Для боротьби зі спуфінгом приймачі GNSS повинні «виловлювати» підроблені сигнали з суміші автентич-

них і підроблених сигналів. Після того, як супутниковий сигнал позначено як підроблений, він може бути виключений з розрахунку позиціонування [17].

Різні країни інвестують кошти в забезпечення стійкості GNSS до підробок, створюючи систему безпеки безпосередньо на своїх супутниках. З системою OS-NMA (Open Service Navigation Message Authentication – Відкритий сервіс аутентифікації навігаційних послань) Galileo стала першою супутниковою системою, яка вводить службу захисту від спуфінгу безпосередньо на цивільному сигналі GNSS. OS-NMA – це безкоштовний сервіс на частоті Galileo E1. Він дозволяє аутентифіціювати навігаційні дані на супутниках Galileo і навіть на супутниках GPS. Такі навігаційні дані несуть інформацію про місцезнаходження супутника і в разі їх зміни приведуть до неправильного обчислення розташування приймача. В даний час OS-NMA знаходиться в розробці, але її планується зробити загальнодоступною в найближчому майбутньому. GPS експериментує з новою системою аутентифікації Chimera [17]. У роботі [18] розроблено алгоритм виявлення спуфінгу на основі апріорних знань об положеннях групи супутників. Алгоритм передбачає використання нейронної мережі на базі MLP- класифікаторів. **Ніколас Гатсіс, Давід Акопян із** UTSA Department of Electrical and Computer Engineering розробили алгоритм визначення атаки на електричні мережі та системи СНС. Але принцип дії алгоритму не опубліковано [19].

Всі наведені вище дослідження в області протидії спуфінгу розраховані на: використання достатньо вартісного обладнання, спеціалізованих «вумних» антен зі спеціалізованим програмним забезпеченням на базі новітніх методів інформаційних технологій, у тому числі нейронної мережі. Однак немає прикладів розробки засобів боротьби без достатньо вартісних змін у конфігурації СНС обладнання.

Мета дослідження – розробка алгоритму виявлення впливу спуфінгу під час виконавчої прокладки. Пропонується розробити алгоритм виявлення спуфінгу засобами ЕКНІС із можливостями усунення його наслідків. Після імплементування програмної реалізації алгоритму soft-девелоперами, передбачається оновлення програмного забезпечення бортового ЕКНІС при заході в порт, де є їх представники.

Виклад матеріалу дослідження. Запропонований алгоритм (рис. 2) вимагає відсутність криволінійного маневру протягом плеча маршруту та нульовий/незначний градієнт швидкості течії/вітру. Дані GPS постійно (в середньому раз у 5 секунд, як відображає їх ЕКНІС Transas NaviSailor 4000) заносяться до масиву group протягом часу timer1, значення якого встановлює оператор ЕКНІС. Якщо протягом цього часу є зависання показників GPS, згідно порівняння із параметром $timer2 \in (0; timer1]$, тоді додатково видається відповідно сповіщення про сбій системи позиціонування GPS. Масив group має розмірність timer1*60/5 рядків та 3 стовпчики (1 , 2 – довгота та широта, 3 – швидкість SOG, шаг дискретизації дорівнює step_GPS, тобто це частота відображення ЕКНІС даних позиції з GPS). Дані потрібні для формування локального тренду позицій судна за час timer1.

На базі локального тренду з даних масиву group математично визначаються координати його кінцевої точки, яка є наступною точкою массиву trend для подальшої побудови основного тренду від WPT1 (way point) до WPT2/WOL2 (wheel over line). Якщо алгоритм визначає вплив спуфінгу: розраховується відхилення теоретичної позиції щодо плеча поточного/наступного (обирається найближче при опусканні перпендикулярів на вказані плечі), для побудови маршруту повернення використовується інтерактивний інструмент як Curve heading line у Transas NaviSailor 4000; далі дані заносяться до БД для відправки у відповідні організації.

При визначенні статусу позиції здійснюється порівняння теоретичної позиції за побудованим трендом массиву даних trend та позицією GPS(яка під впливом спуфінгу може співпадати із лінією плеча) та плечем маршруту. Якщо є відхилення теоретичної позиції з лінії тренду по відношенню до лінії плеча, тоді статусом буде наявність впливу спуфінгу.

Якщо присутні АІС цілі є доцільним визначити їх геокоординати. На базі порівняння даних САРП та АІС здійснити відповідні висновки. Крім того, при наявному спуфінгу, геокоординати таких цілей будуть однаковими, що є додатковою ознакою для алгоритму, оскільки спуфінг не діє вибірково, а судна-жертви будуть під впливом з ймовірністю прямо пропорційній їх відстані до спуферу.

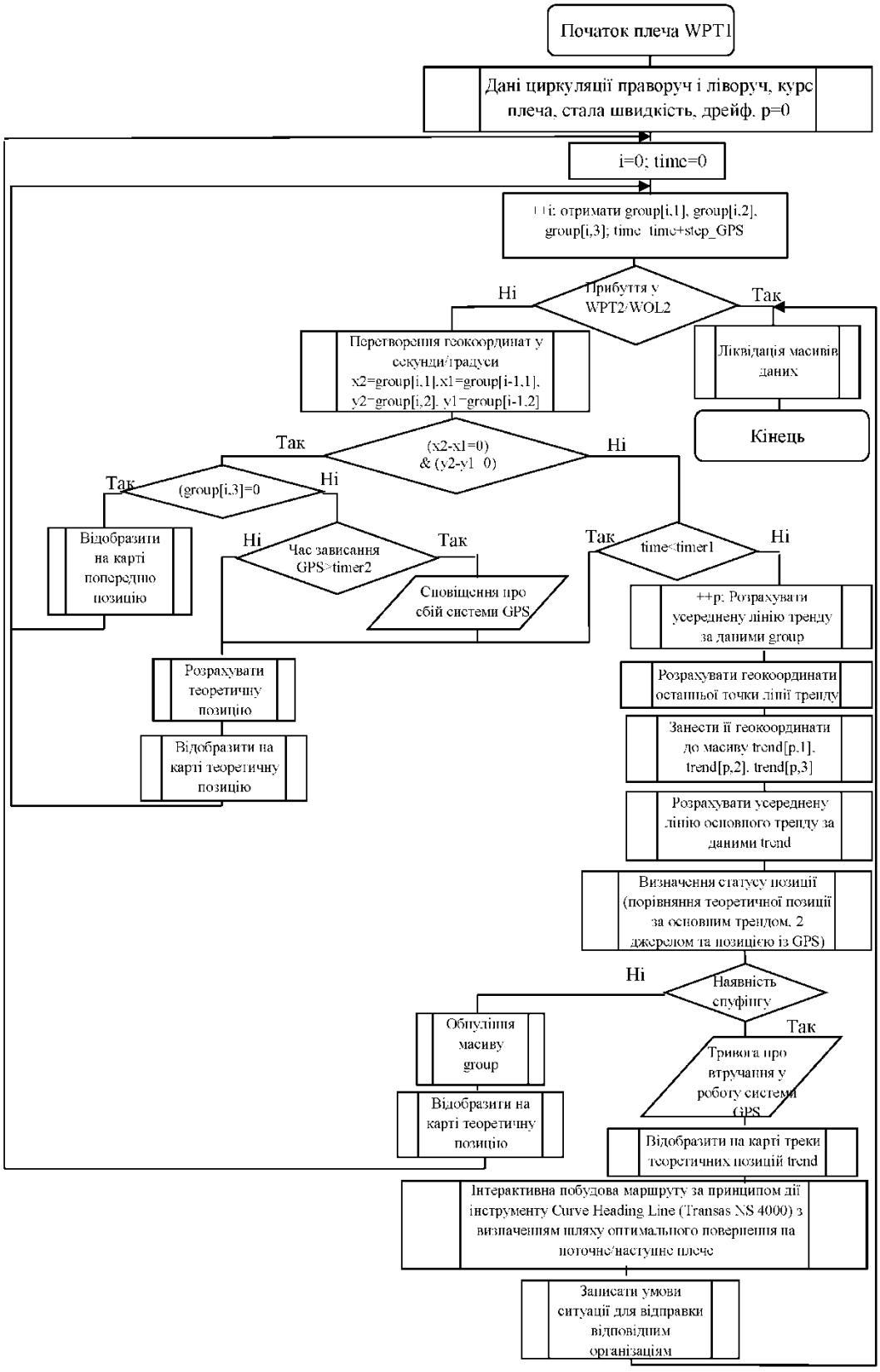

Рис. 2. Алгоритм виявлення спуфінгу засобами ЕКНІС

Висновки. У роботі надано алгоритм визначення спуфінг-атаки з розрахуванням приблизної позиції і пропонуванням маршруту найскорішого повернення на поточне/наступне плече маршруту. Оскільки є обмеження доцільності використання алгоритму: наявність незначного градієнту або нульовий градієнт швидкості течії/вітру на плечі маршруту та прямолінійність плеча, у подальшому, можлива розробка алгоритму визначення такого типу атак при поворотах судна. Також можливе накладання при перевірці маршруту шару карти випадків нападу піратів, або схожих випадків спуфінгу для більш деталізованого аналізу при визначенні ознак спуфінгу.

СПИСОК ЛІТЕРАТУРИ:

1. Подделка письма электронной почты почти от любого человека менее чем за 5 минут и способы защиты. *Режим доступу:* https://habr.com/ru/company/cloud4y/blog/341096/
2. Подделать адрес отправителя в e-mail. *Режим доступу:* https://xakep.ru/2014/03/05/easy-hack-182/
3. Подделка писем. Защита. *Режим доступу:* https://habr.com/ru/company/cbs/blog/314738/
4. Американские аналитики: Россия намеренно искажает сигналы GPS. *Режим доступу:* http://seafarers.com.ua/russian-gps-spoofing/16149/
5. Проблема подмены навигационного сигнала. *Режим доступу:* https://glonassgps.com/novie-sluchai-podmeny-gps-signala-v-rossii
6. Mass GPS Spoofing Attack in Black Sea? *Режим доступу:* https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea
7. TOI: сбои в работе GPS в Израиле произошли из-за России. *Режим доступу:* https://cont.ws/@contemplator/1375625
8. *Above Us Only Stars. SPOOFING* ACTIVITY ACROSS *RUSSIA*, CRIMEA, AND *SYRIA. Режим доступу:*
9. https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf
10. Report: Russian GPS Spoofing Threatens Safety of Navigation. *Режим доступу:*
11. https://www.maritime-executive.com/editorials/report-russian-gps-spoofing-threatens-safety-of-navigation
12. Norway says it proved Russian GPS interference during NATO exercises. *Режим доступу:* https://www.reuters.com/article/us-norway-defence-russia/norway-says-it-proved-russian-gps-interference-during-nato-exercises-idUSKCN1QZ1WN
13. Ведущие страны отказываются от GPS в пользу радиолокации из-за риска хакерских атак. *Режим доступу:*
14. http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:GPS#.D0.A1.D0.BE.D0.B7.D0.B4.D0.B0.D0.BD_.D0.BD.D0.BE.D0.B2.D1.8B.D0.B9_.D0.B0.D0.BB.D0.B3.D0.BE.D1.80.D0.B8.D1.82.D0.BC_.D0.B4.D0.BB.D1.8F_.D0.B7.D0.B0.D1.89.D0.B8.D1.82.D1.8B_.D0.BE.D1.82_GPS-.D1.81.D0.BF.D1.83.D1.84.D0.B8.D0.BD.D0.B3.D0.B0
15. НАВИГАЦИЯ 2.0: КАК ОБМАНЫВАЮТ GPS И ВОССТАНАВЛИВАЮТ ИСТИНУ. *Режим доступу:* https://www.computerra.ru/183473/gps-spoofing/
16. Тодд Хамфрис. Как обмануть GPS. *Режим доступу:* https://www.ted.com/talks/todd_humphreys_how_to_fool_a_gps/transcript?language=ru
17. Спуфинг-атака на GPS-системы может сбить маршрут пользователя. *Режим доступу:* https://www.anti-malware.ru/news/2018-07-16-1447/26837
18. 'Spoofed' GPS signals can be countered, researchers show. *Режим доступу:* http://news.cornell.edu/stories/2012/07/researchers-counter-gps-spoof-attacks
19. Защита от спуфинг-атак на координатно-временные системы. *Режим доступу:* http://vestnik-glonass.ru/news/corp/zashchita-ot-spufingatak-na-koordinatnovremennye-sistemy/
20. Рубцов Н.С. Алгоритм защиты от спуфинга аппаратуры потребителей спутниковых навигационных систем // Известия ТулГУ. Технические науки. 2018 (4). С.92-101. *Режим доступу:* https://cyberleninka.ru/article/v/algoritm-zaschity-ot-spuffinga-apparatury-potrebiteley-sputnikovyh-navigatsionnyh-sistem
21. Как защитить ГНСС от спуфинга. *Режим доступу:* http://vestnik-glonass.ru/news/tech/kak-zashchitit-gnss-ot-spufinga/
22. New UTSA study presents method to stop cyber attacks on GPS-enabled devices. *Режим доступу:* http://www.utsa.edu/today/2018/03/story/GPS-spoofing.html

АЛГОРИТМ ОПРЕДЕЛЕНИЯ ВЛИЯНИЯ СПУФИНГА ВО ВРЕМЯ ИСПОЛНИТЕЛЬНОЙ ПРОКЛАДКИ ПРОГРАММНЫМИ СРЕДСТВАМИ ЭЛЕКТРОННОЙ КАРТОГРАФИЧЕСКОЙ НАВИГАЦИОННО-ИНФОРМАЦИОННОЙ СИСТЕМЫ

Петровский Андрей Валерьевич,
кандидат технических наук, доцент, доцент кафедры судовождения и электронных навигационных систем Херсонской государственной морской академии, г. Херсон, Украина, e-mail: andreyanybody@gmai.com,
ORCID ID: 0000-0002-3337-9577

Анотація. Целью статьи является разработка алгоритма выявления влияния спуфинга при исполнительной прокладке. Предлагается разработать алгоритм выявления спуфинга электронной картографической навигационно-информационной системою с возможностями устранения его последствий. После имплементирования программной реализации алгоритма soft-девелоперами, предусматривается обновление программного обеспечения бортовой электронной картографической навигационно-информационной системы при заходе в порт, где есть их представители. В процессе исследования использованы методы исследования: эмпирические (сравнение) и теоретические (анализ и синтез) с использованием теории навигации, информационных систем и алгоритмов, особенностей электронных картографических систем.

Основные результаты исследования. Разработанный алгоритм основан на анализе трека позиций судна. Все позиции трека в настоящее время бортовой электронной картографической навигационно-информационной системой устанавливаются на электронную карту при выборе оператором соответствующего режима, но не отслеживаются и не анализируются. На основе полученных географических координат позиций формируется тренд, который оценивает возможность работы устройства под контролем при сравнении тренда и данных из другого источника позиционирования, если оно есть, например с Echo reference или Estimated position с данными приборов GPS | DGPS. Если произошло значительное отклонение, алгоритм рассчитывает маршрут возвращения на ближайшее плечо маршрута с использованием соответствующих инструментов электронной картографической навигационно-информационной системы. В случае их отсутствия – предоставляется рекомендованный перечень географических координат для ручного построения маршрута возвращения.

Научная новизна. Поскольку последние исследования и решения поставленных вопросов противодействия спуфингу осуществлялись в разрезе установки дополнительного оборудования и признания необходимости наличия у штурмана более распространенных знаний из области теории радиосигналов, предоставленный алгоритм облегчит определение моментов внешнего контроля судового оборудования GPS | DGPS программными средствами и станет основой для дальнейших исследований по решению этой проблемы для коммерческого и пассажирского транспорта. Практическая значимость достигается в нескольких направлениях: нет необходимости в дополнительном образовании штурманов по теории радиосигналов – достаточно стандартной подготовки; есть возможность определять момент времени захвата контроля; осуществляется автоматизированное построение в интерактивном режиме маршрута возвращения на выбранное плечо маршрута, в случае значительного отклонения истинной позиции судна по данным проведенной обсервации/другого источника позиционирования и анализа трека от позиции по данным GPS|DGPS; пополнение базы данных соответствующих организаций для выпуска Admiralty Information Overlay с целью повышения внимания штурманов в данном районе.

Ключевые слова: *электронная картографическая навигационно-информационная система, спуфинг, алгоритм, GPS.*

ALGORITHM FOR DETERMINING THE INFLUENCE OF SPOFING DURING THE EXECUTIVE LAYING BY THE SOFTWARE OF THE ELECTRONIC CARTOGRAPHIC NAVIGATION-INFORMATION SYSTEM

Petrovskiy Andrii Valeriyovich,
Candidate of Technical Sciences, Associate Professor, Associate Professor of Department of Navigation and Electronic Navigation Systems, Kherson State Maritime Academy, Kherson, Ukraine, e-mail: andreyanybody@gmai.com,
ORCID ID: 0000-0002-3337-9577

Abstract. The aim of the article is to develop an algorithm for identifying the impact of spoofing during executive laying. It is proposed to develop an algorithm for detecting spoofing by an electronic cartographic navigation and information system with the possibilities of eliminating its consequences. After implementing the software implementation of the algorithm by soft developers, it is planned to update the software of the on-board electronic cartographic navigation and information system when entering the port where there are representatives. In the research process, research methods were used: empirical (comparison) and theoretical (analysis and synthesis) using the theory of navigation, information systems and algorithms, and features of electronic cartographic systems.

The main results of the research. The developed algorithm is based on the analysis of the track position of the vessel. All track positions are currently installed on-board electronic cartographic navigation and information system on an electronic map when the operator selects the appropriate mode, but is not tracked and analyzed. Based on the obtained geographical coordinates of the positions, a trend is formed that evaluates the possibility of the device working under control when comparing the trend and data from another source of positioning, if any, for example, with Echo reference or Estimated position with data from GPS devices | DGPS. If a significant deviation has occurred, the algorithm calculates the return route to the nearest route shoulder using the appropriate tools of the electronic cartographic navigation and information system. In case of their absence, a recommended list of geographical coordinates is provided for the manual construction of a return route.

Scientific novelty. Since the latest research and solutions to the issues raised to counteract spoofing were carried out in the context of installing additional equipment and recognizing the need for the navigator to have more common knowledge in the field of radio signal theory, the algorithm provided will facilitate the determination of the moments of external control of ship GPS equipment | DGPS software tools and will become the basis for further research to solve this problem for commercial and passenger vehicles. Practical significance is achieved in several directions: there is no need for additional training of navigators in the theory of radio signals – standard training is enough; it is possible to determine the time point of control capture; automated construction of the return route to the selected route arm in the interactive mode is carried out in the event of a significant deviation of the vessel's true position according to the observational data / other positioning and analysis source of the track from the position according to GPS | DGPS data; updating the database of relevant organizations for the release of Admiralty Information Overlay in order to increase the attention of navigators in this area.

Keywords: *electronic cartographic navigation and information system, spoofing, algorithm, GPS.*

REFERENCES:

1. Poddelka pisma elektronnoj pochty pochti ot lyubogo cheloveka menee chem za 5 minut i sposoby zashhity. Rezhim dostupu: https://habr.com/ru/company/cloud4y/blog/341096/
2. Poddelat adres otpravitelya v e-mail. Rezhim dostupu: https://xakep.ru/2014/03/05/easy-hack-182/
3. Poddelka pisem. Zashhita. Rezhim dostupu: https://habr.com/ru/company/cbs/blog/314738/
4. Amerikanskie analitiki: Rossiya namerenno iskazhaet signaly GPS. Rezhim dostupu: http://seafarers.com.ua/russian-gps-spoofing/16149/
5. Problema podmeny navigaczionnogo signala. Rezhim dostupu: https://glonassgps.com/novie-sluchai-podmeny-gps-signala-v-rossii

6. Mass GPS Spoofing Attack in Black Sea? Rezhim dostupu: https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea
7. TOI: sboi v rabote GPS v Izraile proizoshli iz-za Rossii. Rezhim dostupu: https://cont.ws/@contemplator/1375625
8. Above Us Only Stars. SPOOFING ACTIVITY ACROSS RUSSIA, CRIMEA, AND SYRIA. Rezhim dostupu: https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf
9. Report: Russian GPS Spoofing Threatens Safety of Navigation. Rezhim dostupu: https://www.maritime-executive.com/editorials/report-russian-gps-spoofing-threatens-safety-of-navigation
10. Norway says it proved Russian GPS interference during NATO exercises. Rezhim dostupu: https://www.reuters.com/article/us-norway-defence-russia/norway-says-it-proved-russian-gps-interference-during-nato-exercises-idUSKCN1QZ1WN
11. Vedushhie strany otkazyvayutsya ot GPS v polzu radiolokaczii iz-za riska khakerskikh atak. Rezhim dostupu: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:GPS#.D0.A1.D0.BE.D0.B7.D0.B4.D0.B0.D0.BD_.D0.BD.D0.BE.D0.B2.D1.8B.D0.B9_.D0.B0.D0.BB.D0.B3.D0.BE.D1.80.D0.B8.D1.82.D0.BC_.D0.B4.D0.BB.D1.8F_.D0.B7.D0.B0.D1.89.D0.B8.D1.82.D1.8B_.D0.BE.D1.82_GPS-.D1.81.D0.BF.D1.83.D1.84.D0.B8.D0.BD.D0.B3.D0.B0
12. Navigacziya 2.0: kak obmany vayut GPS I vosstanavlivayut istinu. Rezhim dostupu: https://www.computerra.ru/183473/gps-spoofing/
13. Todd Khamfris. Kak obmanut GPS. Rezhim dostupu: https://www.ted.com/talks/todd_humphreys_how_to_fool_a_gps/transcript?language=ru
14. Spufing-ataka na GPS-sistemy mozhet sbit marshrut pol zovatelya. Rezhim dostupu: https://www.anti-malware.ru/news/2018-07-16-1447/26837
15. 'Spoofed' GPS signals can be countered, researchers show. Rezhim dostupu: http://news.cornell.edu/stories/2012/07/researchers-counter-gps-spoof-attacks
16. Zashhita ot spufing-atak na koordinatno-vremennye sistemy. Rezhim dostupu: http://vestnik-glonass.ru/news/corp/zashchita-ot-spufingatak-na-koordinatnovremennye-sistemy/
17. Rubczov N.S. Algoritm zashhity ot spufinga apparatury potrebitelej sputnikovykh navigaczionnykh sistem// Izvestiya TulGU. Tekhnicheskie nauki. 2018 (4). S.92-101. Rezhim dostupu: https://cyberleninka.ru/article/v/algoritm-zaschity-ot-spuffinga-apparatury-potrebiteley-sputnikovyh-navigatsionnyh-sistem
18. Kak zashhitit GNSS ot spufinga. Rezhim dostupu: http://vestnik-glonass.ru/news/tech/kak-zashchitit-gnss-ot-spufinga/
19. New UTSA study presents method to stop cyber attacks on GPS-enabled devices. Rezhim dostupu: http://www.utsa.edu/today/2018/03/story/GPS-spoofing.html