УДК 004.056.55

М. В. ЄСІНА, І. Д. ГОРБЕНКО, д-р техн. наук

ВИКОРИСТАННЯ СИСТЕМИ GPS У БАГАТОФАКТОРНІЙ АВТЕНТИФІКАЦІЇ

Вступ

В наш час у технологічно розвинених державах проблемам кібернетичної безпеки приділяється особлива увага.

Стосовно даної проблематики розроблюється та впроваджується достатня кількість міжнародних стандартів. Одним з таких стандартів є стандарт ISO/IEC 19790, який прийнято і в Україні (ДСТУ ISO/IEC 19790).

Забезпечення безпеки інформаційної системи є одним з найважливіших завдань в ході її експлуатації, тому що від конфіденційності, цілісності та доступності інформаційних ресурсів залежить швидкість прийняття рішень, ефективність і надійність роботи.

Суттєво важливою послугою з безпеки інформації є послуга доступності. Її можна трактувати як суттєві труднощі в отриманні доступу порушниками та зловмисниками до інформації, які роблять спроби несанкціонованого доступу (НСД).

Задача захисту від НСД стоїть на одному з перших місць при проектуванні та експлуатації інформаційних систем. В якості одного із способів захисту від НСД можна розглядати процедуру багатофакторної автентифікації. Процедура багатофакторної автентифікації може включати в себе два та більше фактори. При цьому ці фактори можуть використовуватись у довільному порядку та у довільній комбінації. Варіанти вибору факторів та їх комбінації залежать від інформації, що обробляється і зберігається у інформаційній системі, та від самої системи.

Зважаючи на важливість проблеми захисту від НСД на міжнародному рівні прийнято ряд стандартів відносно захищеності засобів криптографічного захисту від НСД. У першу чергу до них необхідно віднести стандарт ДСТУ ISO/IEC 19790, що визначає вимоги безпеки для криптографічних модулів. В ньому визначено чотири рівні безпеки. Безумовною вимогою на четвертому рівні є застосування захисту від НСД на основі методів та механізмів багатофакторної автентифікації [1, 3, 5].

Загальні принципи багатофакторної автентифікації

Спочатку надамо загальні визначення.

Автентифікація – це процедура чи процес встановлення достовірності твердження, що суб’єкт або об’єкт має заявлені (очікувані) властивості.

Багатофакторна автентифікація – це автентифікація з хоча б двома незалежними факторами автентифікації. При її реалізації можуть використовуватись фактори різної природи
[3, 6].

Загальну схему процедури ідентифікації та автентифікації користувача при його доступі до інформаційної системи наведено на рис. 1 [9].

Механізми автентифікації пов’язані із захистом інформації від її модифікації, підміни чи створення хибної. Самі механізми автентифікації можна розглядати як заходи захисту, які призначені для встановлення достовірності передачі повідомлення чи відправника або засобів верифікації санкціонування індивіда для отримання конкретних категорій інформації, а також як методи захисту в ІТС від різних видів обману її користувачів.

До переваг багатофакторної автентифікації можна віднести здатність захистити інформацію, як від внутрішніх загроз, так і від зовнішніх вторгнень.

Слабкістю багатофакторної автентифікації можна вважати необхідність використання додаткових програмно-апаратних комплексів, засобів зберігання і зчитування даних [4].

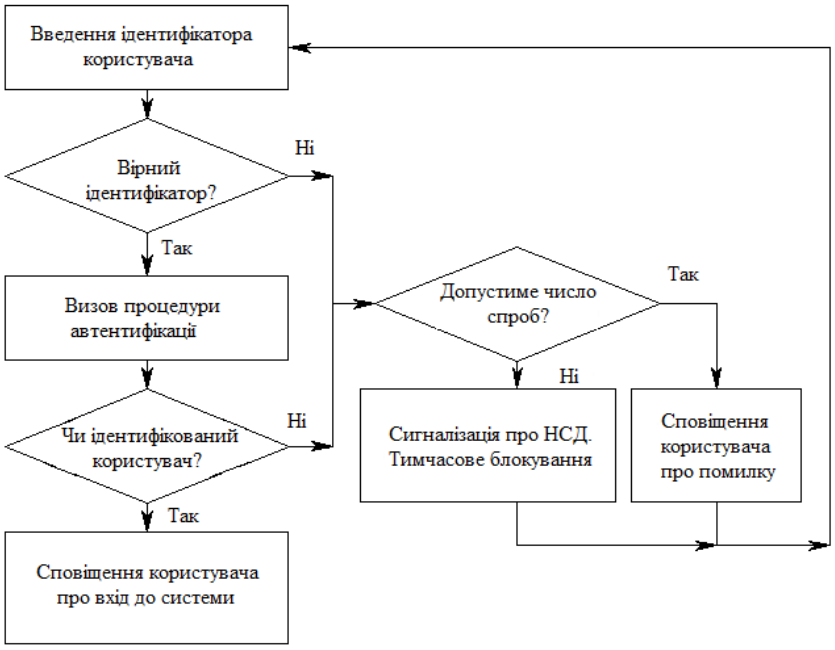

Рис. 1. Класична процедура ідентифікації та автентифікації

Методи автентифікації класифікують згідно засобам, що використовуються. Наведемо наступну класифікацію [3, 6, 9 – 10]:

- знання – інформація, яку має суб'єкт, вона дозволяє йому отримати доступ до ресурсів системи чи деякої секретної інформації (пароль чи пін-код);
- володіння – річ, яку має суб'єкт (електронна або магнітна картка, флеш-пам'ять, електронний ключ);
- властивість, яку має суб'єкт (біометричні характеристики – статичні і динамічні);
- місцезнаходження – координати місця, де знаходиться суб'єкт (GPS координати).

Перші три вказані методи використовуються досить давно і є поширеними. Останній метод тільки починає розвиватись та розповсюджуватись. Його застосування стало можливим завдяки використанню навігаційних систем GPS (Global Positioning System). Дані, отримані про суб'єкта з її допомогою, а саме місце розташування, можуть слугувати ідентифікатором при автентифікації [10].

Загальний опис GPS систем

GPS складається з 24 супутників, положення яких на орбіті завжди точно відомо. Кожен супутник передає безперервний потік ідентифікуючої інформації, яка при об'єднанні з сигналами від інших видимих супутників дозволяє точно визначати географічне місце знаходження.

Загальний принцип використання системи – визначення місця розташування шляхом виміру моментів часу прийому синхронізованого сигналу від навігаційних супутників антеною користувача. Для визначення тривимірних координат, GPS-приймач повинен мати наступну інформацію: $\left|x-a_j\right|=c(t_j-\tau)$, де: a_j – місцезнаходження j-го супутника, t_j – момент часу прийому сигналу від j-го супутника за годинником користувача, τ – невідомий момент часу синхронного випромінювання сигналу усіма супутниками за годинником користувача, c – швидкість світла, x – невідоме тривимірне розташування користувача.

GPS складається з трьох основних сегментів: космічного, управляючого та користувацького. Супутники GPS транслюють сигнал з космосу і всі GPS-приймачі використовують цей сигнал для обчислення свого положення у просторі за трьома координатами в режимі реального часу [11].

Кожен супутник системи GPS передає унікальну послідовність сигналів, яка надходить у приймач у цілком певний момент часу. У загальному випадку GPS-приймач може використовувати сигнали супутника безпосередньо для обчислення свого географічного розташування. Він може перевірити свої результати, скориставшись так званим диференціальним GPS-методом, і при цьому часто збільшується точність. У відповідності з цією методикою географічне місце розташування обчислюється шляхом аналізу сигналів від різних супутників [7].

Модель спостережень просторових географічних координат від супутникової радіонавігаційної системи можна представити у наступному вигляді:

$$\begin{cases} z_{\lambda i} = \lambda_i + \varepsilon_{\lambda i} \\ z_{\gamma i} = \gamma_i + \varepsilon_{\gamma i} \end{cases}, \quad (1)$$

де λ_i – географічна довгота, γ_i – географічна широта, $\varepsilon_{\lambda i}$ та $\varepsilon_{\gamma i}$ – шуми спостережень, відповідно за довготою та широтою, з дисперсією $\sigma^2{}_{\lambda i}$ та $\sigma^2{}_{\gamma i}$ [12].

Типова точність визначення координат GPS-приймачами в горизонтальній площині складає близько 1-2 метрів (за умови гарної видимості небосхилу). Точність визначення висоти над рівнем моря звичайно в 2-5 разів нижча за точність визначення координат у тих же умовах (тобто в ідеальних умовах 2-10 метрів). Головним фактором, що впливає на зниження точності GPS, є неповна видимість небосхилу (у межах великих міст дана ситуація досягається за рахунок знаходження GPS-приймача в умовах щільної міської забудови).

Точність визначення координат при знаходженні транспортного засобу на відкритій місцевості та при русі великими автомобільними шляхами буде складати 1-2 метри. При русі вузькими вулицями, особливо, коли близько розташовані будівлі, точність складатиме 4-10 метрів. При знаходженні автомобіля досить близько до висотних будівель, точність може спадати до 20-30 метрів.

У самій системі глобального позиціонування закладена помилка у 15-20 метрів, яку не може виправити жоден алгоритм. У сумі усі зазначені помилки можуть створити похибку розміром до декількох метрів [13].

Автентифікація з використанням GPS систем

Розглянемо спочатку метод автентифікації, з використанням GPS координат, у загальних аспектах [9].

Новим напрямком автентифікації є доказ достовірності віддаленого користувача за його місцезнаходженням. Даний захисний механізм засновано на використанні системи космічної навігації типу GPS.

Користувач, що має апаратуру GPS, багаторазово посилає координати заданих супутників, що знаходяться в зоні прямої видимості. Підсистема автентифікації, знаючи орбіти супутників, може з точністю до метра визначити місце розташування користувача. Висока надійність автентифікації визначається тим, що орбіти супутників схильні до коливань, передбачити які досить важко. Крім того, координати постійно змінюються, що зводить нанівець можливість їх перехоплення.

Складність злому системи полягає в тому, що апаратура передає оцифрований сигнал супутника, не виконуючи жодних обчислень. Всі обчислення про місцезнаходження виконуються на сервері автентифікації.

Апаратура GPS проста і надійна у використанні і порівняно недорога. Це дозволяє використовувати її у випадках, коли авторизований віддалений користувач повинен знаходитися у потрібному місці.

Опишемо детально механізм автентифікації за допомогою GPS-координат [7].

У середині 1990-х років групою дослідників з Колорадо була розроблена методика застосування диференційного GPS-методу для дистанційного визначення відмінностей між різними фізичними точками в просторі. Основна ідея проілюстрована на рис. 2 [7].

Є два суб'єкти – А і В, які приймають сигнали від супутників системи GPS. Суб'єкт А приймає GPS-сигнали в певній послідовності, яка залежить від відстані до супутника. Він може прийняти і відкорелювати ці дані, а потім передати їх суб'єкту В.

Суб'єкт В приймає ті ж самі GPS-дані від тих же супутників, але в інші моменти часу, оскільки супутники знаходяться від нього на інших відстанях, ніж від А. Якщо В відповідним чином скорелює GPS-сигнали, то зможе обчислити, як дані повинні були б прийматися в тому місці, де знаходиться А, в конкретний момент часу. Якщо GPS-дані, послані йому А, збігаються з очікуваними В GPS-даними, то він може бути впевненим, що повідомлення від А передаються з того місця, яке В очікував. Об'єднані GPS-дані залежать як від часу, так і від місця розташування.

Таким чином, В точно знає, що повідомлення надійшло з географічного розташування А, навіть якщо насправді не відомо, чи сам А відправив його. Але цього достатньо для багатьох закритих додатків, зокрема, тих, які виконуються на спеціально виділених комп'ютерах у фізично захищених місцях.

Для того щоб сфальсифікувати інформацію про місцезнаходження А, зловмисник повинен мати можливість отримати GPS-дані, які отримував би сам А. Потім він повинен відкорелювати ці дані так само, як, за пропозицією В, це зробив би А, і відправити їх йому зі строго визначеними часовими параметрами. Так як GPS-дані є часозалежними, то підробка атакуючої сторони достовірна лише обмежений період часу. На практиці атакуюча сторона просто не здатна зібрати необхідну інформацію і вчасно передати її жертві, щоб успішно замаскуватися під інший комп'ютер.

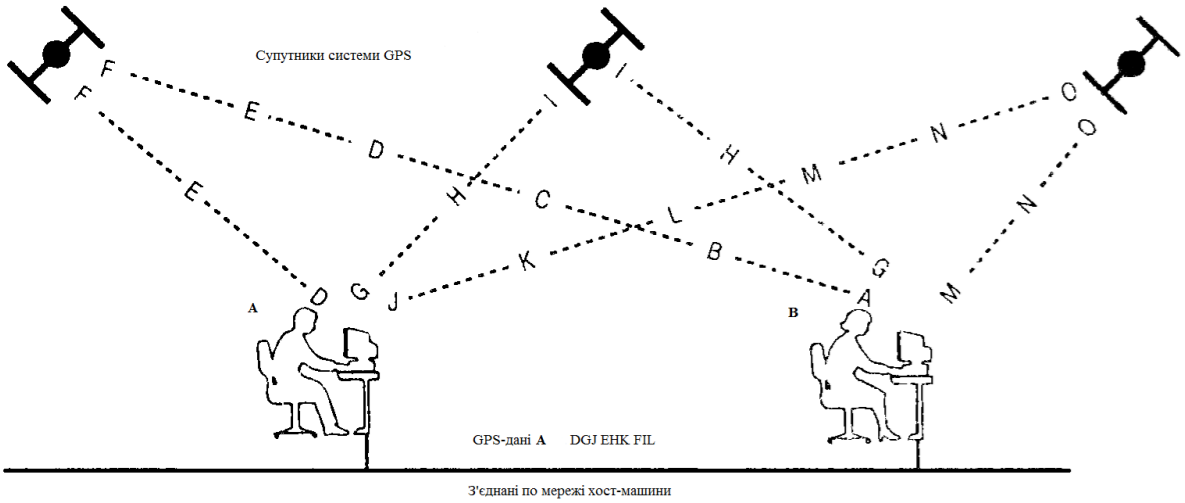

Рис. 2. Концепція автентифікації по місцю розташування з використанням системи GPS

Однак даній технології притаманні і певні недоліки. По-перше, потрібна антена, здатна приймати GPS-сигнали від декількох супутників, хоча більшості стандартних GPS-приймачів необхідно приймати сигнали тільки від двох або трьох супутників. По-друге, методика працює тільки в тому випадку, якщо відправник та отримувач можуть «бачити» однакові супутники. По-третє, є ризик вторгнення в приватне життя, так як автентифікуюча інформація ідентифікує місце знаходження джерела даних. Якщо дані не шифруються, то людина або організація, що проводять аналіз сигналів, можуть зв'язати дані з фізичним місцезнаходженням їхнього джерела.

Відносний ризик полягає і в передачі фальшивих GPS-сигналів. Супутники системи GPS передають сигнал, який зрозумілий простим громадянським приймачам, і існує ймовірність моделювання сигналів від декількох GPS-супутників. Теоретично, подібні сигнали могли б

обдурити GPS-автентифікатор за місцем розташування, особливо якщо атакуюча сторона одночасно використовує ще й переналаштований нею комп'ютер, який намагається себе автентифікувати. Однак, добре спроектований GPS-автентифікатор, можливо, буде працювати правильно і в умовах завад, оскільки використовує максимально можливу кількість супутникових сигналів, а генератор завад не може заглушити всі видимі GPS-сигнали.

Таким чином, хоча автентифікація за місцем розташування за допомогою системи GPS є багатообіцяючою, необхідно ще накопичувати певний досвід, щоб сказати, наскільки добре вона працює в умовах реальних операційних потреб і різних атак [7].

Використання автентифікації на основі GPS координат у багатофакторній автентифікації

Важливим питанням є оцінка безпеки схем багатофакторної автентифікації. В процесі побудови системи захисту від НСД спочатку необхідно визначити перелік факторів, які можна використовувати для здійснення багатофакторної автентифікації. Для захисту від НСД до інформації та ресурсів з використанням певних факторів автентифікації необхідно визначити повний перелік атак зі сторони існуючих чи потенційних криптоаналітиків (порушників), зробити їх класифікацію, вибрати критерії та показники, які дозволили б порівняти їх та вибрати такі атаки, які можуть бути реалізовані та забезпечували б досягнення максимальних значень ймовірностей НСД [2].

Найсильнішою схемою автентифікації є багатофакторна автентифікація, яка поєднує в собі використання різноманітних методів.

Як основні показники захисту від НСД можна визначити такі [2]:

1. $P_{НСД}(n)$ – ймовірність НСД у n спробах, де n – кількість спроб отримати НСД;
2. $t_б$ – безпечний час;
3. $\Delta T = T_Д$ – допустимий час НСД;
4. n – кількість спроб, які можливо здійснити.

Аналіз використання схем багатофакторної автентифікації показує, що в ході їх побудови можуть використовуватися механізми з послідовним, паралельним або комбінованим з'єднанням елементів, які реалізують фактори автентифікації. Також кількість елементів у схемі може змінюватися, вона буде залежати від призначення системи, що захищається, та вимог до неї [6].

У випадку використання в багатофакторному механізмі автентифікації двох факторів можливі такі комбінації: пароль(і) та ключ(і), пароль(і) та біометрична ознака(и), ключ(і) та біометрична ознака(и), координати GPS та пароль(і), координати GPS та ключ(і), координати GPS та біометрична ознака(и).

Розглянемо комбіновану схему багатофакторної автентифікації із паралельно-послідовним з'єднанням елементів, коли можливе використання декількох факторів – паролів, біометричних ознак, ключів, координат GPS тощо. Така схема багатофакторної автентифікації зображена на рис. 3.

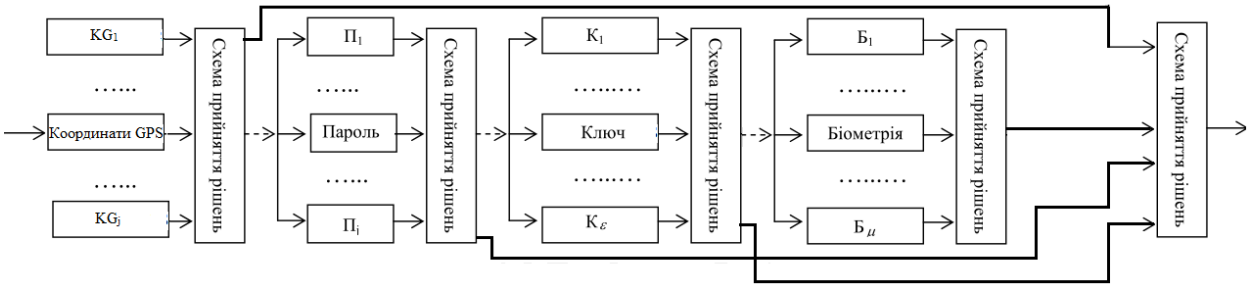

Рис. 3. Комбінована схема багатофакторної автентифікації

Також практичне значення мають окремі випадки, коли застосовується один або два фактори автентифікації у послідовному з'єднанні [8]. На рис. 4 зображена схема послідовного з'єднання двофакторного механізму автентифікації «координати GPS і ключ».

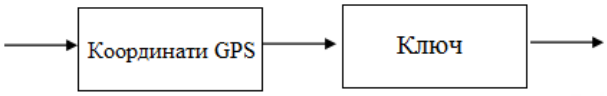

Рис. 4. Схема послідовного з'єднання двофакторного механізму захисту від НСД «координати GPS і ключ»

При використанні автентифікації на основі координат GPS потрібно використовувати деякий криптографічний протокол автентифікації. Під криптографічним протоколом автентифікації будемо розуміти криптографічний протокол встановлення достовірності твердження, що об'єкт (суб'єкт) має очікувані властивості.

У якості такого протоколу можна використовувати протоколи, що наведені у відповідних стандартах з інформаційної безпеки (наприклад, ISO/IEC 9798-2:2008 (E), ДСТУ ISO/IEC 9798-4:2005 (Проект)).

Використаємо в якості протоколу автентифікації механізм автентифікації з двома проходами із ISO/IEC 9798-2:2008 (E). Наведемо загальний опис цього механізму.

У цьому механізмі автентифікації унікальність/своєчасність контролюється генерацією та перевіркою мітки часу або порядкових номерів (див. Додаток Б ISO/IEC 9798-1: 1997).

Механізм автентифікації проілюстровано на рис. 5.

Рис. 5. Механізм 3 – автентифікація з двома проходами

Форма маркеру ($Token_{AB}$), що посилається об'єктом А об'єкту В, ідентична тій, яка вказується у п. 6.1.1 стандарту:

$$Token_{AB} = Text_2 \| e_{K_{AB}}\left(TN_A \| I_B \| Text_1\right) \tag{2}$$

Форма маркеру ($Token_{AB}$), що посилається об'єктом В об'єкту А, наступна:

$$Token_{BA} = Text_4 \| e_{K_{AB}}\left(TN_B \| I_A \| Text_3\right) \tag{3}$$

Включення розпізнавального ідентифікатору I_B до $Token_{AB}$ та включення розпізнавального ідентифікатору I_A до $Token_{BA}$ є необов'язковим.

Розпізнавальний ідентифікатор I_B включається до $Token_{AB}$ для попередження повторного використання $Token_{AB}$ від об'єкта А зловмисником, під виглядом об'єкту В. З аналогічних причин розпізнавальний ідентифікатор I_A присутній в $Token_{BA}$. Їх включення виконується необов'язково, тому що у середовищах функціонування, де такі атаки не можуть виникати, один з них або обидва можуть бути опущені. Розпізнавальні ідентифікатори I_A та I_B можуть також бути опущені, якщо використовуються односпрямовані ключі.

Вибір з використання або мітки часу, або порядкових номерів у цьому механізмі залежить від можливостей позивача і перевіряючого, а також середовища функціонування.

Нижче описується Механізм 3 – автентифікація з двома проходами:

(1) А генерує та посилає $Token_{AB}$ В.

(2) Після отримання повідомлення, що містить $Token_{AB}$, В перевіряє $Token_{AB}$ дешифруванням зашифрованої частини, а потім перевіряє правильність розпізнавального ідентифікатору I_B, якщо він присутній, а також мітку часу або порядковий номер.

(3) В генерує та посилає $Token_{BA}$ А.

(4) Повідомлення на стадії (3) оброблюється способом, аналогічним стадії (2) п. 6.1.1 стандарту.

У випадку з використанням автентифікації на основі GPS координат у якості $Token_{AB}$ будуть виступати GPS координати місця розташування об'єкту А, а у якості $Token_{BA}$ виступатиме відповідь об'єкта В на отримані від А координати.

Висновки

Стандарт ISO/IEC 19790 встановлює вимоги безпеки для криптографічних модулів, що використовуються в системі безпеки для захисту критичної інформації. Головною вимогою безпеки Рівня Захисту 4 є застосування багатофакторної автентифікації.

В якості основних факторів автентифікації можна використовувати: властивість суб'єкту; знання суб'єкту; володіння суб'єкту; місцезнаходження суб'єкту.

Для кожного із факторів автентифікації необхідно визначити повний перелік атак зі сторони атакуючих чи потенційних криптоаналітиків (порушників), сформулювати критерії та показники, які дозволили б їх порівняти та обрати такі атаки, які можуть бути реалізовані та забезпечували б досягнення максимальних значень ймовірностей НСД, потім сформулювати пропозиції та рекомендації, в тому числі для застосування у механізмах багатофакторної автентифікації.

Всі вище вказані фактори, окрім фактора місцезнаходження, є поширеними. Метод автентифікації суб'єкта за його місцезнаходженням тільки починає розвиватись. Як і всі методи, він має свої недоліки та переваги.

До переваг можна віднести:

– координати GPS постійно змінюються, що зводить нанівець можливість їх перехоплення;
– складність злому системи полягає в тому, що апаратура передає оцифрований сигнал супутника, не виконуючи жодних обчислень;
– апаратура GPS проста і надійна у використанні і порівняно недорога.

У якості недоліків можна вказати:

– необхідність антени, яка може приймати GPS-сигнали від декількох супутників;
– цей метод працює тільки в тому випадку, якщо відправник і одержувач «бачать» однакові супутники;
– є ризик вторгнення в приватне життя;
– відносний ризик полягає в передачі фальшивих GPS-сигналів.

Для забезпечення надійного захисту даних, що передаються між компонентами системи GPS по незахищеним каналам передачі даних, необхідно використовувати засоби криптографічного захисту інформації. Наприклад, при реалізації процедури автентифікації за допомогою GPS координат необхідно використовувати протоколи автентифікації, що визначені відповідними міжнародними стандартами.

Список літератури: 1. *Горбенко, І.Д.* Прикладна криптологія. Теорія. Практика. Застосування / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Форт, 2012. – 870 с. 2. *Горбенко, І.Д.* Прикладна криптологія / І.Д. Горбенко, Ю.І. Горбенко. – Харків : Форт, 2012. – 868 с. 3. *Єсіна, М. В.* Багатофакторна автентифікація: використання механізмів двофакторної автентифікації для захисту від несанкціонованого доступу / М. В. Єсіна, І. Д. Горбенко // Компьютерное моделирование в наукоемких технологиях (КМНТ-2014) : Тр. науч.-техн. конф. с междунар. участием, 28-31 мая 2014 г. – Харьков : Харьк. нац. ун-т им. В.Н. Каразина, 2014. – С. 159–162. 4. *Єсіна, М.В.* Метод захисту інформації на основі багатофакторної автентифікації: GPS координати як фактор автентифікації // IV Міжнар. наук.-техн. конф. "Захист інформації і безпека інформаційних систем", 04 – 05 червня 2015 р. – Львів : Нац. ун-т "Львівська політехніка", 2015. – С. 121 – 122. 5. Інформаційні технології – Методи забезпечення безпеки – Вимоги до безпеки для криптографічних модулів (ISO/IEC 19790:2012(E)): ДСТУ ISO/IEC 19790. – [Чинний від 2012-08-15]. – К. : Держспоживстандарт України, 2012. – 98 с. – (Національні стандарти України). 6. *Симонс, Г.Д.* Обзор методов аутентификации информации. – М. : ТИИЭР, 1988. – Т. 76, №5. – С. 105 – 125. 7. *Смит, Р. Э.* Аутентификация: от паролей до открытых ключем : пер. с англ. – М. : Изд. дом «Вильямс», 2002. – 432 с. 8. *Столлингс, В*. Криптография и защита сетей. Принципы и практика / В. Столлингс. – 2-е изд. – М. : Вильямс, 2001. – 672 с. 9. [Режим електронного доступу]: http://sernam.ru/ss_23.php 10. [Режим електронного доступу]: http://www.webtoall.ru/library/2035/ 11. [Режим електронного доступу]: https://ru.wikipedia.org/wiki/GPS 12. [Режим електронного доступу]: http://conf-ulstu.ru/aaa_18.php 13. [Режим електронного доступу]: http://sts-51.ru/index.php/navigatsiya/materials-about/73-fort-news3.

Харківський національний
університет радіоелектроінки

Надійшла до редколегії 18.04.2015