УДК 004.056

Г.М. ГУЛАК[*], П.М. СКЛАДАННИЙ[**]

ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ АВТОМАТИЗОВАНИХ СИСТЕМ ПЕРЕРОБКИ ІНФОРМАЦІЇ Й УПРАВЛІННЯ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ

[*]Інститут проблем математичних машин і систем НАН України, м. Київ, Україна
[**]Державний університет телекомунікацій, м. Київ, Україна

Анотація. *Для забезпечення гарантоздатності автоматизованих систем переробки інформації та управління безпілотними літальними апаратами у статті запропоновано застосування криптосхеми, яка реалізує шифр багатоалфавітної заміни на основі алгоритму генерації підстановок заміни на базі псевдовипадкової послідовності. Криптосхема включає блок контролю (виявлення атак) на модуль криптографічного захисту інформації. Запропонована відносна оцінка ефективності системи захисту, яка може бути використана для визначення припустимості застосування деяких проектних рішень для побудови системи безпеки.*
Ключові слова: *БПЛА, імітостійкість, автентифікація, атака, багатоалфавітна заміна.*

Аннотация. *Для обеспечения гарантоспособности автоматизированных систем переработки информации и управления беспилотными летательными аппаратами в статье предложено применить криптосхему, реализующую шифр многоалфавитной замены на базе алгоритма генерации подстановок замены из псевдослучайной последовательности. Криптосхема включает блок контроля (выявления атак) на модуль криптографической защиты информации. Предложена относительная оценка эффективности системы защиты, которая может использоваться для определения допустимости использования отдельных проектных решений при построении системы безопасности.*
Ключевые слова: *БПЛА, имитостойкость, аутентификация, атака, многоалфавитная замена.*

Abstract. *A detailed analysis of the reliability of automated systems of processing information and controlling unmanned aerial vehicles was carried out; the relevance of use and protection issues is disclosed in this paper. The actual directions of researches, concerning safety of radio systems of control and UAV data were determined. A cipher of multi-alphabetical substitutions on the basis of the algorithm for generating replacement substitutions on the basis of gamma, which is obtained by block encryption, as well as a cryptographic circuit, that includes the control unit (detection of attacks) on the cryptographic tool information protection were proposed in the paper. The relative estimation of the efficiency of the radio link protection systems of the UAV was proposed. This gives an opportunity to estimate the appropriateness of one or other design solutions for security.*
Keywords: *UAV, imitation resistance, authentication, attack, multi-alphabetical substitutions.*

1. Вступ

У різних сферах суспільного життя всього світу для вирішення завдань цивільного та військового спрямування стрімко поширюється застосування безпілотних літальних апаратів (БПЛА). БПЛА використовуються військовими формуваннями, підрозділами охорони суспільного правопорядку та подолання надзвичайних ситуацій тощо для виконання завдань, в яких отримання інформації звичайними засобами утруднене або ж наражає на небезпеку для здоров'я та навіть життя людей. Інформація, зібрана бортовими засобами БПЛА, передається споживачеві у реальному часі або зберігається на борту в вигляді масиву даних [1].

Про актуальність дослідження наукових проблем побудови та застосування БПЛА свідчить той факт, що, за нашими підрахунками, тільки у Російській Федерації (РФ) протягом 2010–2016 років опубліковано понад 350 науково-дослідних робіт, присвячених різним аспектам їх побудови та підвищення ефективності застосування. Зокрема, у роботі [2] визначені завдання, які вирішуються робототехнічними комплексами (включаючи безпілотні

літальні апарати) військового призначення в інтересах ракетних військ і артилерії Сухопутних військ (СВ) РФ. У роботі [3] запропоновано концепцію створення комплексів для виявлення і боротьби з малогабаритними БПЛА в інтересах тактичної ланки СВ РФ. У роботі [4] розглянуті актуальні питання забезпечення інформаційної безпеки БПЛА тактичної ланки, при цьому основна увага приділена захисту інформації при використанні яких апаратів. Остання робота також становить інтерес з точки зору оцінки спеціалістів РФ реальної вразливості сучасних БПЛА щодо атак із застосуванням технологій кібернетичного ураження автоматизованих систем.

Останні події в зоні проведення антитерористичної операції свідчать про існування проблеми практичного забезпечення гарантоздатності автоматизованих систем переробки інформації та управління БПЛА, оскільки Збройні сили України зіткнулися з частими випадками втрати контролю і управління над своїми БПЛА, основною причиною яких є застосування спеціальних засобів моніторингу частотного діапазону, створення інформаційних перешкод і перехоплення безпілотних апаратів [5]. Можна відмітити, що відомі факти проведення атак на канали управління [6], які призводять до порушення режиму їх штатного функціонування та навіть перехоплення неушкоджених БПЛА, внаслідок чого їх власники зазнають суттєвих матеріальних та моральних збитків, а супротивник отримує досить непогані «трофеї».

Тому актуальним постає питання щодо формування вимог та рекомендацій стосовно раціональної системи захисту інформації в радіоканалах БПЛА, що виконують завдання в інтересах збройних сил та правоохоронних органів, з урахуванням специфічних загроз та потенційно можливих наслідків їх реалізації.

Слід зазначити, що останнім часом спостерігається стале зростання кількості спроб несанкціонованого втручання (кібернетичних атак) в роботу автоматизованих систем переробки інформації та управління критично важливими об’єктами інфраструктури (АСУ КВОІ), внаслідок чого органи державного та військового управління, суб’єкти господарювання державного та приватного секторів економіки мають величезні збитки, а суспільство опиняється на межі як локальних, так і глобальних техногенних катастроф. Тому метою даної роботи є розробка та обґрунтування побудови схеми захисту, яка повинна виключати можливості непередбачуваних змін системи та послуг, що надаються (атрибут гарантоздатності – цілісність, інакше – імітостійкість), а також неавторизованого доступу до інформації про послуги (атрибут гарантоздатності – конфіденційність) [7].

2. Аналіз останніх публікацій. Вразливості АСУ та вихідні припущення

Проблемі підвищення безпеки функціонування автоматизованих систем присвячено безліч науково-практичних досліджень, включаючи нормативні, методологічні та технічні аспекти криптографічного й технічного захисту інформації. Значний внесок у формування наукового підґрунтя для побудови безпечних систем зробили провідні вітчизняні та зарубіжні вчені: Коваленко І.М., Бабаш А.В., Глухов М.М., Горбенко І.Д., Діффі У., Зубов А.Ю., Хеллман М., Хорошко В.О., Шанкин Г.П., Шеннон К. та багато інших. Серед зарубіжних досліджень вже була згадана робота [4], в який серед актуальних напрямів досліджень відмічені такі:

– захист конфіденційності потоків даних при інформаційному обміні з БПЛА та безпека від нав’язування неправдивої інформації;

– створення засобів криптографічного захисту критичної інформації, що мають низьке енергоспоживання і відповідають суворим вимогам щодо зовнішніх впливів. Серед умов розв’язку означеної задачі визначена висока ймовірність компрометації критичної інформації, яка зберігається або циркулює у бортовій системі управління БПЛА, та ін.

Слід зауважити, що переважна більшість відповідних досліджень стосовно убезпечення АСУ КВОІ присвячена проблемам захисту інформації щодо якої законодавчо визна-

чена відповідальність за впровадження власником автоматизованої системи відповідного комплексу нормативно-організаційних та інженерно-технічних заходів. У той же час, на законодавчому рівні статус інформації, що циркулює у БПЛА, не визначений, відсутні конкретні вимоги та норми щодо її захисту.

Значна частина дослідників проблем безпеки АСУ звертає увагу на те, що їх вразливості обумовлені поширеним застосуванням як транспортні мережі радіоканалів зв'язку або систем зв'язку загального доступу (включаючи фізичний або логічний доступ) до мережі Інтернет, а також використання для побудови елементів системи управління поширених операційних систем сімейства Windows, мережевих протоколів стеку TCP/IP тощо, оскільки відповідні технології, механізми та засоби поряд з достатньо розвиненою функціональністю в певних умовах застосування можуть утворювати приховані канали деструктивного впливу на потоки даних та команд управління або сприяти витоку інформації з обмеженим доступом.

Слід зауважити, що, на відміну від БПЛА цивільного застосування, системам управління яких загрозу становлять переважно чинники природного та техногенного характеру, для БПЛА, що виконують завдання в інтересах збройних сил та правоохоронних органів, особливу небезпеку мають фактори антропогенного характеру, обумовлені намаганнями відповідних військових або кримінальних сил порушити штатне функціонування бортового комплексу апаратури або ліквідувати (захопити) БПЛА.

Використання засобів радіозв'язку (радіоканалів) для управління БПЛА та отримання інформації від них підвищує ризики несанкціонованого втручання в їх роботу.

Виходячи з визначених умов та вимог нормативних документів [8], можна вважати, що потенційний порушник системи безпеки є або порушником корпоративного типу (другий рівень), який має змогу створення спеціальних технічних засобів та програмного забезпечення, вартість яких співвідноситься з можливими фінансовими збитками, що виникатимуть від порушення конфіденційності, цілісності та підтвердження авторства інформації, зокрема, при втраті, спотворенні та знищенні інформації, яка захищається; або порушником, що має науково-технічний ресурс, який прирівнюється до науково-технічного ресурсу спеціальної служби економічно розвинутої держави (третій рівень).

З урахуванням вразливості та доступності радіоканалів БПЛА логічно вважати, що порушник:

– знає протоколи зв'язку, алгоритми автентифікації та шифрування, але не знає діючого ключа;

– може перехоплювати всі команди та інформаційні потоки від БПЛА завдяки доступу до радіоканалу, а також без суттєвої затримки із застосуванням засобів радіоелектронної боротьби заглушувати радіоканали від легального центру управління БПЛА та нав'язувати фіктивні команди (імітація).

Слід зауважити, що необхідну інформацію порушник може отримувати внаслідок аналізу відносно неушкоджених блоків управління БПЛА, що були збиті засобами вогневого ураження.

Комплекс управління БПЛА за призначенням поділяється на два сегменти: бортовий комплекс управління (БКУ) і наземний комплекс управління (НКУ).

Завданнями БКУ є:

– рішення завдання навігації і автоматичного керування літальним апаратом;

– забезпечення командно-телеметричної взаємодії з НКУ;

– забезпечення функціонування корисного навантаження;

– забезпечення самодіагностики літального апарата.

Основними завданнями НКУ є:

– забезпечення командно-телеметричної взаємодії з БКУ;

– забезпечення ручного управління в реальному часі;

– надання елементів програмування і управління БПЛА;

– подання телеметричної інформації у графічному вигляді;

– відображення даних корисного навантаження.

Внаслідок атаки на автоматизовану систему управління БПЛА можуть бути порушені конфіденційність та цілісність команд і даних, які передаються з борта БПЛА, що дає можливість маніпуляцій з ними.

3. Вибір методу захисту

Слід зазначити, що шифрування інформації за методом гамування завдяки атакам за допомогою відомого (повністю або з деякою ймовірністю) відкритого тексту є вразливим щодо спроб нав'язування фіктивних команд [9].

Загалом придатними методами забезпечення імітозахисту [10] радіоканалів можна вважати такі (таблиця 1):

1. Використання відміток часу (ВВЧ).

2. Зміну ключів шифрування за «плаваючим» графіком (ПЗК).

3. Впровадження електронного цифрового підпису (ЕЦП).

4. Використання кодів автентифікації повідомлень (англ. message authentication code – MAC).

5. Застосування імітостійкого шифрування за допомогою псевдовипадкової послідовності підстановок заміни: $X_1, X_2, ..., X_1, ...$ – шифру багатоалфавітної заміни (БАЗ).

Електронний цифровий підпис є, з одного боку, найбільш безпечним методом контролю цілісності повідомлень та підтвердження авторства, з іншого, його застосування є проблематичним внаслідок обчислювальної складності його математичних процедур, які можуть призвести до зменшення пропускної здатності радіоканалу управління. Певною проблемою також є застосування сертифікатів відкритих ключів від довіреної сторони.

Виходячи з переваг та недоліків різних методів захисту, зокрема, враховуючи, з одного боку, певні недоліки перших трьох із наведених методів, з іншого – якості БАЗ в аспекті забезпечення імітостійкості та безпеки у разі повторення ключа шифрування уявляється доцільним для убезпечення радіоканалу скористатися саме цим механізмом.

У роботі [11] нами був розроблений та досліджений швидкий алгоритм формування послідовності підстановок заміни (ПЗ) на основі рівномірно розподіленої псевдовипадкової двійкової послідовності (РРПВП). При цьому показано, що раціональний розмір підстановки заміни дорівнює 16. Тобто генеровані підстановки мають вид:

$$X = \begin{matrix} 0 & 1 & 2 & & D & E & F \\ x_0 & x_1 & x_2 & \cdots & x_D & x_E & x_F \end{matrix}.$$

Таблиця 1. Порівняльний аналіз методів протидії підробці повідомлень та/або контролю цілісності

№	Метод	Переваги	Недоліки
1	ВВЧ	Не суттєво збільшує довжину повідомлення. Не потребує суттєвих витрат часу процесора	Потребує стійкого шифрування повідомлень. Потребує чутливої процедури синхронізації годинників приймача та передавача. Потрібна велика розрядність цифрового годинника для забезпечення малої ймовірності підробки
2	ПЗК	Не змінює виробничої потужності системи	Не суттєво підвищує імітостійкість. Ускладнює процедури управління ключами

Продовж. табл. 1

3	ЕЦП	Практично неможливо підробити ЕЦП, що побудоване на основі сучасних алгоритмів. Дозволяє будувати системи з юридично значущим доведенням авторства повідомлення	Має відносно тривалий час формування/перевірки ЕЦП. ЕЦП коротких повідомлень може мати довжину, що суттєво перевищує їх розмір; Потрібно мати 3 ключі: секретний для шифрування, секретний і відкритий для формування /перевірки ЕЦП. Потребує наявності в системі третьої сторони – центру сертифікації ключів
4	*MAC*	Для перевірки цілісності даних потрібен один секретний ключ. Ймовірність підробки *MAC* не перевищує величини 2^{-M}, де M – його довжина	У випадку забезпечення конфіденційності повідомлень за допомогою симетричних БШ потрібно мати два ключі: шифрування та формування *MAC*. Генерація *MAC* за допомогою алгоритму блокового шифрування потребує значного часу
5	БАЗ	Має високу швидкодію порівняно з іншими методами КЗІ. Зберігає стійкість при повторенні ключа шифрування	Генерація псевдовипадкової послідовності (ПВП) підстановок заміни: X_1, X_2, ... зменшує загальну швидкодію. Відмова блоку генерації ПВП у разі несанкціонованого втручання у роботу системи може зруйнувати систему безпеки

На основі РРПВП, що генерується за допомогою сучасного стандарту алгоритму блокового шифрування (стандарти ДСТУ 7624-2014, AES тощо), пропонується побудувати схему шифру БАЗ.

На рис. 1 представлена відповідна криптосхема модуля захисту БКУ радіолінії БПЛА, яка включає:

генератор РРПВП на основі алгоритму шифрування у режимі OFB, що використовує як вхідні дані ключ шифрування *K* та вектор ініціалізації *IV*;

вузол контролю та блокування на основі статистичного критерію «задачі про розладку»;

алгоритм генерації підстановок заміни;

вузол застосування підстановки заміни до чергового шістнадцяткового символу команди або даних.

Зауважимо, що у випадку шифрування за допомогою модуля КЗІ команди управління $K = a_1, a_2, ..., a_L$, яка подана у вигляді послідовності шістнадцяткових чисел довжини L, зловмиснику для нав'язування фіктивної команди $\tilde{K} = b_1, b_2, ..., b_L$, що відрізняється за n позиціями від істинної, у разі випадкового перебору варіантів необхідно зробити $\frac{1}{2}(2^4 - 1)^n = 15^n$ спроб. При цьому ймовірність p_n нав'язування фіктивного варіанта команди управління з першої спроби швидко зменшується з ростом n (таблиця 2):

Таблиця 2. Ймовірності нав'язування команди, що відрізняється від істинної на *n* позиціях

n	1	2	3	4	5	6	7	8
p_n	$6{,}7\cdot10^{-2}$	$4{,}4\cdot10^{-3}$	$3{,}0\cdot10^{-4}$	$2{,}0\cdot10^{-5}$	$1{,}3\cdot10^{-6}$	$8{,}8\cdot10^{-8}$	$5{,}9\cdot10^{-9}$	$3{,}9\cdot10^{-10}$

Для забезпечення необхідної ймовірності угадування кожна команда має доповнюватися контрольною сумою, яка розраховується за алгоритмом *CRC*32, кожна шістнадцяткова цифра якої зашифровується за допомогою БАЗ. У цьому випадку ймовірність угадування з першої спроби дорівнює p_8.

Для виключення можливості послідовного перебору варіантів БКУ після заданої кількості невдалих спроб має блокувати канал управління на певний час та переходити в автономний режим роботи.

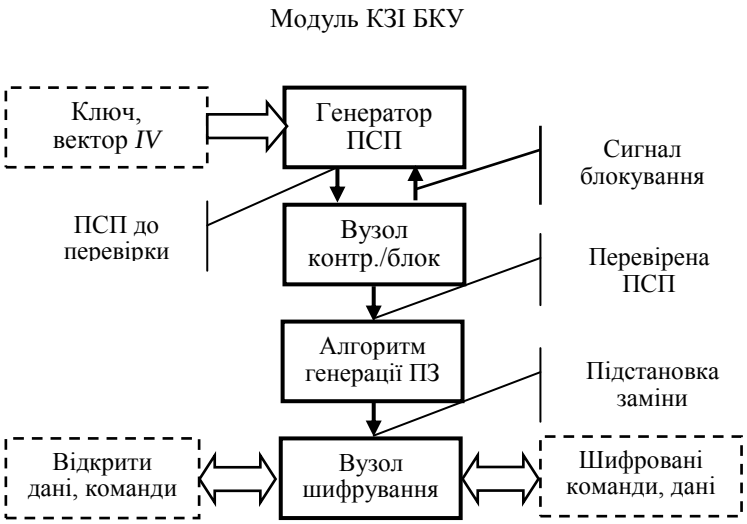

Рис. 1. Криптосхема модуля КЗІ БКУ

З метою виявлення відхилень у роботі модуля КЗІ на основі статистичного критерію «задачі про розладку» [12] введено систему контролю та їх блокування, що забезпечує необхідну для практичних застосувань оперативність реакції. Повторний запуск системи може відбуватися, наприклад, після виходу БПЛА із зони дії засобів атаки на нього. Слід зазначити, що для певних застосувань для підвищення безпеки сигнал виявлення порушення у роботі криптосхеми може бути використаний для формування команди БКУ для переходу БПЛА в автономний режим виконання завдань.

Для виключення можливості маніпуляцій з діючим ключем, який може бути вилучений із пам'яті засобу КЗІ в разі збиття БПЛА, доцільно здійснювати його періодичну заміну за допомогою безпечного протоколу на базі блокового алгоритму шифрування. Зміну необхідно здійснювати шляхом перезапису старого ключа.

4. Критерій оцінки ефективності

Зважаючи на матеріальний характер збитків у разі перехоплення БПЛА внаслідок успішної атаки на БКУ та необхідність певних матеріальних витрат для реалізації атак, про що йшлось під час обговорення моделі порушника, є логічним як оцінку рівня безпеки системи захисту (засобу КЗІ) – величини Q – відносної ефективності системи захисту використовувати відповідне співвідношення, а саме:

$$Q = \frac{p^* \cdot \max(C_ш)}{\min\{C_{A1}, C_{A2}, ..., C_{Ak}\}},$$

де $C_ш$ – очікувана вартість втрат унаслідок атаки, $C_{A1}, C_{A2}, ..., C_{Ak}$ – вартість реалізації відомих атак на систему захисту та їх комбінацій, включаючи криптоаналітичні атаки, атаки

на реалізацію та атаки по побічних каналах, p^* – ймовірність успішної реалізації кращої атаки.

Логічним кроком буде вибір таких границь для відносної ефективності системи захисту:

$Q << 1$– високий рівень безпеки, коли очікувана шкода власника БПЛА суттєво менше витрат порушника на реалізацію атаки;

$Q \approx 1$ – середній рівень безпеки, коли очікувана шкода власника БПЛА практично дорівнює сумі витрат порушника на реалізацію атаки, але сукупність атак може мати більшу ефективність;

$Q >> 1$ – занадто низький рівень безпеки, коли очікувана шкода власника БПЛА суттєво перевищує витрати порушника на реалізацію однієї атаки.

Запропоновану характеристику можна проілюструвати такими показниками. За даними Центру аналізу світової торгівлі зброєю Росія у 2009 році придбала два БПЛА ізраїльського виробництва типу «Searcher Mk.2» загальною вартістю 12 млн доларів США [13]. Таким чином, вартість одного БПЛА перевищує вартість пристроїв оперативного дешифрування відомих криптографічних алгоритмів DES або A5/1, що свідчить про неприпустимість їх застосування для захисту каналів управління згаданого БПЛА. У той же час потрібно звернути увагу на те, що вартість атаки повинна включати вартість іншого обладнання для реалізації атак [6].

5. Висновки

Для забезпечення гарантоздатності системи БПЛА (конфіденційності, цілісності/імітостійкості) запропоновано шифр БАЗ на базі алгоритму генерації підстановок заміни на основі гами, що отримується за допомогою алгоритму блокового шифрування згідно з ДСТУ 7624-2014 в режимі OFB. Ймовірність підміни команди у схемі оцінюється величиною $3{,}9 \cdot 10^{-10}$. Запропонований шифр БАЗ припускає 8-кратне повторення ключа без зниження практичної стійкості шифрування. Запропонована криптосхема включає блок контролю (виявлення атак) на модуль КЗІ на основі статистичного критерію «задачі про розладку», який забезпечує необхідну для практичних застосувань оперативність реакції. Запропонована відносна оцінка ефективності системи захисту радіолінії БПЛА дає можливість орієнтовно оцінити припустимість тих або інших проектних рішень для забезпечення безпеки. Подальші дослідження доцільно продовжити у напрямі вдосконалення критерію оцінки якості системи захисту та системи контролю й блокування засобу у разі його виходу з ладу.

СПИСОК ЛІТЕРАТУРИ

1. Лоскутников А.А. Системы автоматического управления БПЛА / А.А. Лоскутников, Н.С. Сенюшкин, В.В. Парамонов // Молодой учёный. – 2011. – № 9 (32). – С. 56 – 58.
2. Наговицин А.И. Робототехнические комплексы военного назначения, опыт и перспективы их применения в РВиА СВ / А.И. Наговицин, А.Г. Севрюков // Известия Южного федерального округа. – 2016. – № 1 (186). – С. 197 – 210.
3. Годунов А.И. Комплекс обнаружения и борьбы с малогабаритными беспилотными летательными аппаратами / А.И Годунов, С.В. Шишков, Н.К. Юрков // Надежность и качество сложных систем. – 2014. – № 2 (6). – С. 62 – 70.
4. Сашников Т.К. К вопросу обеспечения информационной безопасности беспилотных авиационных систем с летательными аппаратами малого и лёгкого класса в специализированных АСУ / Т.К. Сашников // Журнал T-Comm – Телекоммуникации и транспорт. – 2013. – № 6. – С. 71 – 72.
5. [Електронний ресурс]. – Режим доступу: http://militaryrussia.ru.
6. Радиоэлектронный нож для беспилотника: как взломать и перехватить БПЛА [Электронный ресурс]. – Режим доступа: https://tvzvezda.ru/news/vstrane_i_mire/content/201609120753-8de1.htm.

7. Харченко В.С. Гарантоспособность и гарантоспособные системы: элементы методологии / В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2006. – № 5 (7). – С. 7 – 19.
8. Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації. Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України 20.07.2007 № 141 (у редакції наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 14.12.2015, № 767). Зареєстр. в Міністерстві юстиції України 30.07.2007, № 862/14129.
9. Основи криптографічного захисту інформації: [підруч. для вищ. навч. закл.] / Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. – Вінниця: ВНТУ, 2011. – 198 с.
10. Бабаш А.В. Криптография / А.В. Бабаш, Г.П. Шанкин. – М.: СОЛОН-Р, 2002. – 512 с.
11. Гулак Г. М. Швидкий алгоритм генерації підстановок багатоалфавітної заміни / Г.М. Гулак, В.Л. Бурячок, П.М. Складанний // Захист інформації. – 2017. – № 2. – С. 173 – 177.
12. Гулак Г.М. Модель системи виявлення вторгнень з використанням двоступеневого критерію виявлення мережних аномалій / Г.М. Гулак, В.В. Семко, П.М. Складанний // Сучасний захист інформації. – 2015. – № 4. – С. 81 – 85.
13. [Електронний ресурс]. – Режим доступу: https://vz.ru/society/2013/7/17/641662.html.

Стаття надійшла до редакції 10.09.2017