Відомості про авторів / Сведения об авторах / About the Authors

Гарбуз Сергій Вікторович – ад'юнкт, Національний університет цивільного захисту України, ад'юнкт кафедри «Пожежної та техногенної безпеки об'єктів і технологій»; вул. Чернишевського 94, м. Харків, 61023;

Гарбуз Сергей Викторович – адъюнкт, Национальной университет гражданской защиты Украины, адъюнкт кафедры «Кафедра пожарной и техногенной безопасности объектов и технологий»; ул. Чернышевского 94, г. Харьков, 61023; e-mail: garbuz_88@inbox.ru.

Garbuz Sergey – graduate student, National university of civil protection of Ukraine, graduate student of chair «Fire and technological safety of facilities and technology, st. Chernyshevsky 94, Kharkov, 61023;

Ковалёв Александр Александрович – кандидат технических наук, Национальный университет гражданской защиты Украины, доцент кафедры «Инженерной и аварийно-спасательной техники»; ул. Чернышевского 94, г. Харьков, 61023; e-mail: mralexkovalev@gmail.com.

Ковальов Олександр Олександрович – кандидат технічних наук, Національний університет цивільного захисту України, доцент кафедри «Інженерної та аварійно-рятувальної техніки»; вул. Чернишевського 94, м. Харків, 61023; e-mail: mralexkovalev@gmail.com.

Kovalev Alexander – Candidate of technical sciences, National university of civil protection of Ukraine, associate professor of chair «Engineering and rescue equipment»; st. Chernyshevsky 94, Kharkov, 61023;

Титаренко Андрій Вікторович – кандидат психологічний наук, Національний університет цивільного захисту України, заступник начальника факультету оперативно-рятувальних сил; вул. Чернишевського 94, м. Харків, 61023; e-mail: mralexkovalev@gmail.com.

Титаренко Андрей Викторович – кандидат психологических наук, Национальный университет гражданской защиты Украины, заместитель начальника факультета оперативно-спасательных сил; ул. Чернышевского 94, г. Харьков, 61023; e-mail: mralexkovalev@gmail.com.

Titarenko Andrey – Candidate of psychological science, National university of civil protection of Ukraine, deputy head of the faculty of Operational and rescue forces; st. Chernyshevsky 94, Kharkov, 61023

УДК 004.03:65-574.5

В. І. РУЖЕНЦЕВ, А. П. ПОРВАН, М. А. ПАЩЕНКО

ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ВИЗНАЧЕННЯ ОСЕРЕДКІВ ТОКСИЧНОСТІ БІООБ'ЄКТІВ

Робота присвячена організації захисту інформації в інформаційній системі визначення осередків токсичності водних біооб'єктів для унеможливлення несанкціонованого доступу до даних, що зберігаються в базі даних. Розглянуто основні методи захисту інформації та способи їх реалізації у відомих системах екологічного дистанційного моніторингу. Проаналізовано та обрано, що для забезпечення захисту від несанкціонованого доступу до бази даних, де зберігається вся інформація системи, з інших програмних продуктів та для обміну даними в зашифрованому вигляді використовується AES.

Ключові слова: база даних, водна екосистема, захист інформації, інформаційна система, симетричний алгоритм блочного шифрування.

Вступ. Виявлення та оцінка в короткі терміни екологічного ризику, як найбільш важливого показника при прийнятті рішень, що стосуються охорони навколишнього середовища та екологічної безпеки регіону, в силу своєї інформаційної ємності вимагає застосування спеціальних комп'ютерних рішень. Сучасні темпи розвитку систем екологічного моніторингу багато в чому зумовлюють їх зміст. У свою чергу зберігання інформації, що постійно надходить до таких систем, не може проводитися без такої складової, як захист інформації. А застосування автоматизованих методів і засобів своєчасного виявлення осередків токсичності часто пов'язано з отриманням і обробкою безлічі різних параметрів, які потребують захисту під час роботи. Причому ця проблема є досить складною у зв'язку з великою кількістю наявних параметрів, що відрізняються за видом, структурою і інформативністю, які представлені у системі.

Постановка проблеми та аналіз останніх джерел і публікацій. При розробці інформаційної системи (ІС) визначення осередків токсичності водних об'єктів було виділено такі можливі загрози із зовні, як зміна та вилучення даних, що зберігаються в БД, порушення конфіденційності та викрадення даних при передачі їх на ПК.

Для захисту даних використовують криптографію, яка забезпечує не тільки таємність інформації, що зберігається, але і її справжність [1, 2]. Секретність підтримується шляхом шифрування окремих повідомлень або всього файлу цілком. Справжність інформації підтверджується шляхом шифрування спеціальним шифром, що містить всю інформацію, який перевіряється одержувачем для підтвердження особи автора. Він не тільки засвідчує походження інформації, але і гарантує її незмінність.

Навіть просте перетворення інформації є досить ефективним засобом, що дає можливість приховати її суть від більшості некваліфікованих порушників.

Криптографія на сьогодні є єдиним відомим способом забезпечення таємності і підтвердження достовірності інформації в системах екологічного моніторингу, переданої із супутників [3]. Природа стандарту шифрування даних така, що його алгоритм є загальнодоступним, секретним повинен бути тільки ключ. Причому однакові ключі повинні використовуватися і для шифрування, і для дешифрування інформації.

© В. І. Руженцев, А. П. Порван, М. А. Пащенко. 2015

При наявності простих засобів зберігання і передачі інформації в інформаційних екологічних системах існували і не втратили значення до теперішнього часу такі методи її захисту від навмисного несанкціонованого доступу як обмеження доступу, розмежування доступу, криптографічне перетворення інформації, контроль і облік доступу; законодавчі заходи.

Зазначені методи здійснюються тільки організаційно або за допомогою технічних засобів [4, 5].

З появою автоматизованої обробки інформації в ІС змінився і доповнився новими видами фізичний носій інформації та ускладнилися технічні засоби її обробки.

З ускладненням обробки, збільшенням кількості технічних засобів, що беруть участь в ній, збільшуються кількість і види випадкових впливів, а також можливі канали несанкціонованого доступу. Зі збільшенням обсягів, зосередженням інформації, збільшенням кількості користувачів та іншими зазначеними вище причинами збільшується ймовірність навмисного несанкціонованого доступу до суті інформації. У зв'язку з цим розвиваються старі і виникають нові додаткові методи захисту в інформаційних системах, у тому числі екологічних [6, 7].

При цьому правила здійснення контролю доступу до даних є єдиними існуючими методами для досягнення розглянутих вище вимог щодо індивідуальної ідентифікації.

Найкращою політикою управління доступом є політика "мінімально необхідних привілеїв" [1]. Іншими словами, користувач має доступ тільки до тієї інформації, яка необхідна йому в роботі.

Захист результатів екологічного моніторингу за допомогою шифрування - одне з можливих ефективних рішень проблеми їхньої безпеки. Зашифровані дані стають доступними тільки для того, хто знає, як їх розшифрувати.

Існуючі принципи шифрування полягають в шифруванні тексту за допомогою ключа [8-10]. У традиційних алгоритмах шифрування для кодування і декодування використовувався один і той же ключ, хоча у нових системах з відкритим ключем або асиметричного шифрування ключі парні: один використовується для кодування, інший - для декодування інформації. У такому поєднанні кожен користувач володіє унікальною парою ключів. При реалізації такого алгоритму один користувач, якому потрібно надіслати повідомлення іншому, може зашифрувати повідомлення відкритим ключем останнього. Розшифрувати його зможе тільки власник особистого секретного ключа, тому небезпека перехоплення виключена.

Практичне використання захисного шифрування в системах дистанційного моніторингу поєднує традиційні симетричні і нові асиметричні схеми [11]. Шифрування відкритим ключем застосовується для узгодження секретного симетричного ключа, який потім використовується для шифрування реальних даних. Шифрування забезпечує найвищий рівень безпеки даних. Як в апаратному, так і в програмному забезпеченні застосовуються різні алгоритми шифрування.

Таким чином, організація захисту інформації (ЗІ) в системах дистанційного екологічного моніторингу є актуальним практичним завданням.

Специфіка галузі вимагає вирішення ряду завдань при використанні екологічних ІС. На ринку присутні готові рішення, що використовують для зберігання як картографічних даних до файлової системи, так і результатів моніторингу.

Розглянемо деякі відомі приклади реалізації основних методів ЗІ в ІС екологічного моніторингу.

Існуюча система "Secret Net" заміняє стандартний механізм операційної системи по авторизації користувачів і дозволяє проводити аутентифікацію як за паролем, так і з використанням апаратних засобів посиленої аутентифікації і стандартних сертифікатів. Можливо комбінування способів аутентифікації для досягнення двухфакторної (багатофакторної) аутентифікації. Парольна інформація захищена від перехоплення як при локальному введенні (маскування символів, що вводяться шляхом заміни на «*»), так і при мережевий передачі [12].

Програмні продукти "Код Безпеки" призначені для застосування в складних сучасних ГЕО ІС, де реалізовані можливості інтеграції з корпоративними каталогами користувачів, використовуваної інфраструктурою відкритих ключів, впровадженими системами управління мережею, SIEM-рішеннями і т.п. [13].

Також ЗІ може бути побудований з використанням вузькоспеціалізованих систем ЗІ, що закривають одну або декілька заходів, або з використанням комплексних засобів типу "DallasLock", "Акорд" та подібних їм [14].

Система "Лінтер" призначена для забезпечення максимального захисту та дозволяє проводити авторизацію користувачів, має ядро безпеки, ієрархію прав доступу, мандатний захист, контроль доступу з віддалених станцій, проводить протоколювання роботи та контроль за зберіганням інформації) [15].

Відома система "GIS 6 Secure" дозволяє захист доступу до бази даних "ГІС 6" із зовнішніх програмних продуктів. Програма "GIS 6 Secure" виконує роль проміжної ланки між локальним Клієнтом "ГІС 6" і Сервером бази даних, який обробляє запити користувача в зашифрованому вигляді, звіряє ім'я та пароль з параметрами зовнішнього доступу і після успішного проходження перевірки, дозволяє підключитися безпосередньо до самої бази даних [16].

Основним недоліком розглянутих систем є складність, а часом і неможливість їх інтеграції з комплексами автоматизованої системи управління, в тому числі інтегрувати до розроблених рішень. Якщо довірити зберігання і обробку даних екологічних ІС у реляційних базах даних, які є складовою цих систем, проблема такої інтеграції просто зникає. При цьому зменшується число використовуваних автономних систем, а отже, спрощується адміністрування і управління всім процесом визначення осередків токсичності водних біооб’єктів.

Відомими методами блочних шифрів є шифр TEA (один із самих простих в реалізації), мережа Фейштеля (метод оборотних перетворень тексту, при якому значення, обчислені від однієї з частин тексту, накладається на інші частини) та стандарт AES [17].

Розглянуті приклади захисту інформації, як правило, спеціалізовані і володіють більшою захи-

щеністю і функціональністю. Однак ці системи захисту, побудовані на різновиду, нехай навіть брендових, систем захисту інформації, що створить масу проблем при їх експлуатації.

Мета роботи. Метою роботи є розробка заходів з організації ЗІ для системи визначення осередків токсичності водних біооб'єктів. Для забезпечення захисту в розроблюваній системі пропонується використовувати симетричний алгоритм блочного шифрування (AES).

Організація захисту інформації в системі визначення осередків токсичності біооб'єктів. ІС включає в себе біологічну та технічну підсистеми (рис. 1). Біологічною підсистемою є водна екосистема водоймища або водотік, що їхній стан тестується, та еколог. Технічна підсистема складається із наступних елементів: блока модуля реєстрації інформації – безпілотний літаючий апарат, який розкидає зонди (наземні реєструючи блоки), пристрої контролю, та отримує з них інформацію, модуля обробки інформації, БД, блока аналізу інформації, блока формування звіту та блока виводу інформації. Для захисту від несанкціонованого доступу до бази даних з інших програмних продуктів використаємо симетричний алгоритм блочного шифрування (AES).

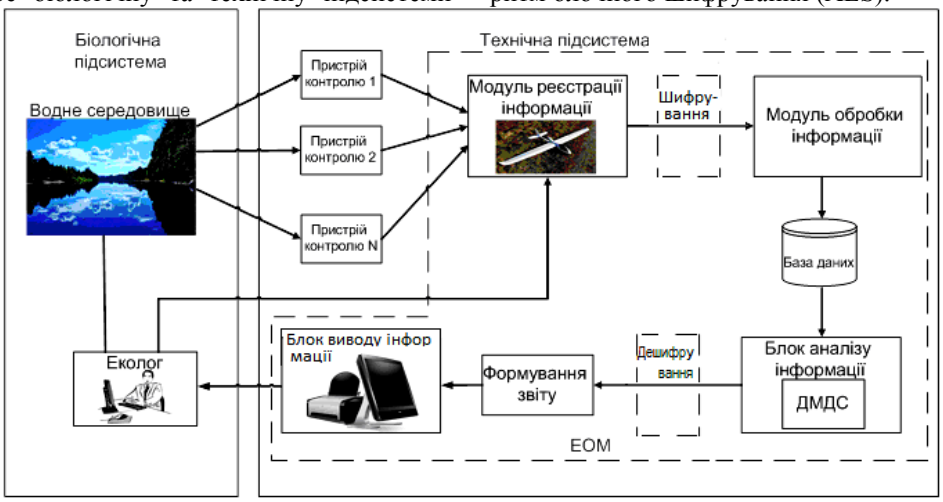

Рис. 1 – Структурна схема інформаційної системи

AES є стандартом, заснованим на алгоритмі Rijndael. Для AES довжина input (блоку вхідних даних) і State (стану) постійна і дорівнює 128 біт, а довжина шифроключа K становить 128, 192, або 256 біт. При цьому, вихідний алгоритм Rijndael допускає довжину ключа і розмір блоку від 128 до 256 біт з кроком в 32 біта. Для позначення обраних довжин input, State і Cipher Key в 32-бітових словах використовується нотація $Nb = 4$ для input і State, $Nk = 4, 6, 8$ для Cipher Key відповідно для різних довжин ключів.

На початку шифрування input копіюється в масив State за правилом:

$$state\,[r,c] = input\,[r+4c],\ \text{для}\ 0 \le r < 4\ \text{і}\ 0 \le c < Nb.$$

Після цього до State застосовується процедура AddRoundKey() і потім State проходить через процедуру трансформації (раунд) 10, 12, або 14 разів (в залежності від довжини ключа), при цьому треба врахувати, що останній раунд дещо відрізняється від попередніх. У підсумку, після завершення останнього раунду трансформації, State копіюється в output за правилом:

$$output\,[r+4c] = state\,[r,c],\ \text{для}\ 0 \le r < 4\ \text{і}\ 0 \le c < Nb.$$

Окремі трансформації SubBytes(), ShiftRows(), MixColumns(), і AddRoundKey() - обробляють State. Масив *w*[] - містить key schedule.

У процедурі SubBytes, кожен байт в state замінюється відповідним елементом у фіксованій 8-бітній таблиці пошуку (1), S; $b_{ij} = S(a_{ij})$.

$$\begin{Vmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{Vmatrix} = \begin{Vmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{Vmatrix} * \begin{Vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{Vmatrix} + \begin{Vmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{Vmatrix} \quad (1)$$

Процедура SubBytes() обробляє кожен байт стану, незалежно виробляють лінійну заміну байтів використовуючи таблицю замін (S-box). Така операція забезпечує лінійність алгоритму шифрування. Побудова S-box складається з двох кроків. По-перше, проводиться взяття зворотного числа в полі Галуа $GF(2^8)$. По-друге, до кожного байта b з яких складається S-box застосовується наступна операція:

$$b_i' = b_i \oplus b_{(i+4)mod8} \oplus b_{(i+5)mod8} \oplus b_{(i+6)mod8} \oplus \oplus b_{(i+7)mod8} \oplus c_i$$

де $0 \le i < 8$, bi є i-ий біт b, а ci - i-ий біт константи $c = 6316 = 99_{10} = 01100011_2$. Таким чином, забезпечується захист від атак, заснованих на простих алгебраїчних властивостях.

У процедурі ShiftRows, байти в кожному рядку state циклічно зсуваються вліво. Розмір зміщення байтів кожного рядка залежить від її номера. `ShiftRows` працює з рядками State. При цій транс-

формації рядка стану циклічно зсуваються на r байт по горизонталі, залежно від номера рядка. Для нульового рядка $r = 0$, для першого рядка $r = 1b$ і т. д. Таким чином кожна колонка вихідного стану після застосування процедури ShiftRows складається з байтів з кожної колонки початкового стану.

У процедурі MixColumns, кожна колонка стану перемножується з фіксованим многочленом $c(x)$.

У процедурі MixColumns, чотири байти кожної колонки State змішуються, використовуючи для цього оборотну лінійну трансформацію. MixColumns обробляє стан по колонках, трактуючи кожну з них як поліном четвертого ступеня. Над цими поліномами виробляється множення в $GF(2^8)$ по модулю x^4+1 на фіксований многочлен $c(x) = x^3+x^2+x+2$. Разом з ShiftRows, MixColumns вносить дифузію в шифр.

У процедурі AddRoundKey, кожен байт стану об'єднується з RoundKey використовуючи операцію XOR (⊕).

У процедурі AddRoundKey, RoundKey кожного раунду об'єднується зі State. Для кожного раунду Round Key виходить з CipherKey використовуючи процедуру KeyExpansion; кожен RoundKey такого ж розміру, що й State. Процедура виробляє побітовий XOR кожного байту State з кожним байтом RoundKey.

Для обробки ключа необхідно провести такі дві процедури: алгоритм розширення ключа та алгоритм вибору раундового ключа (ключа ітерації).

Алгоритм розширення ключа. AES алгоритм, використовуючи процедуру Key Expansion () і подаючи до неї Cipher Key, K, отримує ключі для всіх раундів. Всього виходить $Nb * (Nr + 1)$ слів: спочатку для алгоритму потрібно набір з Nb слів, і кожному з Nr раундів вимагається Nb ключових набору даних. Отриманий масив ключів для раундів позначається як $w[i]$, $0 \le i < Nb*(Nr+1)$.

Алгоритм KeyExpansion(). Функція SubWord() бере чотирьохбайтове вхідне слово і застосовує S-box до кожного з чотирьох байтів. Те, що вийшло, подається на вихід. На вхід RotWord () подається слово $[a_0, a_1, a_2, a_3]$ яке вона циклічно переставляє і повертає $[a_1, a_2, a_3, a_0]$. Масив слів, постійний для даного раунду, $R_{con[i]}$, містить значення $[x^{i-1}, 00, 00, 00]$, де x = {02}, а x^i є ступенем x в $GF(2^8)$ (i починається з 1).

Перші Nk слів розширеного ключа заповнені Cipher Key. У кожне наступне слово, $w[i]$, кладеться значення отримане при операції XOR $w[i-1]$, і $w[i-Nk]$, ті XOR'а попереднього і на Nk позицій раніше слів. Для слів, позиція яких кратна Nk, перед XOR'ом до $w[i-1]$ застосовується трасформації, за якою слідує XOR з константою раунду $Rcon[i]$. Зазначена вище трансформація складається з циклічного зсуву байтів в слові $(RotWord())$, за якою слідує процедура SubWord () - те ж саме, що і SubBytes (), тільки вхідні і вихідні дані будуть розміром в слово.

Важливо зауважити, що процедура KeyExpansion () для 256 бітного Cipher Key трохи відрізняється від тих, які застосовуються для 128 і 192 бітних шіфроключей. Якщо $Nk=8$ і $i-4$ кратно Nk, то SubWord () застосовується і для $w[i-1]$, і для XOR'а.

Алгоритм вибору раундового ключа. На кожній ітерації раундовий ключ для i операції AddRoundKey вибирається з масиву $w[i]$ починаючи з елемента $w[Nb*i]$ до $w[Nb*i+1]$.

Висновки. Таким чином, проведений аналіз сучасних тенденцій в організації ЗІ в ІС екологічного моніторингу відображає, що системи піддаються таким видам загроз як несанкціонований доступ до інформації, що зберігається в базах даних, та атаки при обміні даних, які надходять від пристрою, що реєструє спектральні зміни досліджуваного об'єкту.

В якості найбільш ефективного алгоритму ЗІ було обрано симетричний алгоритм блочного шифрування. Застосування цього алгоритму дозволило за рахунок його байт-орієнтованої структури досягти необхідної та достатньої швидкодії виконання операцій шифрування на різних програмних платформах при досить великому обсязі різнорідної інформації та забезпечити конфіденційність важливої інформації на усіх етапах визначення осередків токсичності біооб'єктів

Список літератури:**1.** *Симмонс, Г. Д.* Обзор методов аутентификации информации [Текст] / *Г. Д. Симмонс*. – ТИИЭР. – 2008. – Т. 76, No 5.**2.** *Уолкер, Б. Дж.* Безопасность ЭВМ и организация их защиты [Текст] / *Б. Дж. Уолкер, Я. Ф. Блейк*. – М.: Связь, 2000.**3.** *Хоффман, Л.* Современные методы защиты информации [Текст] / *Л. Хоффман*. – М.: «Советское радио», 2007.**4.** *Жидких, А. Д.* Теоретические основы компьютерной безопасности [Текст] / *А. Д. Жидких* // Журн. «Обучающая система». – 2011. – No 1. – С. 185-186.**5.** *Грушо, А. А.* Теоретические основы защиты информации [Текст] / *А. А. Грушо, Е. Е. Тимонина.* – М.: Издательство Агентства «Яхтсмен», 1996. **6.** *Варфоломеев, А. А.* Методы криптографии и их применение в банковских технологиях [Текст] / *А. А. Варфоломеев, М. Б. Пеленицын.* – М.: МИФИ, 2006.**7.** *Винокуров, А.* Криптография [Текст] / *А. Винокуров* // Журн. «INFUSED BYTES». – 2009.**8.** *Винокуров, А. Ю.* Еще раз про ГОСТ [Текст] / *А. Ю.Винокуров.* – М.: Монитор. – 2005. – 45 с.**9.** *Баричев, С.* Криптография без секретов [Текст] / *С. Баричев.* – М.: Москва. – 2008. **10.** *Варфоломеев, А. А.* Управление ключами в системах криптографической защиты банковской информации [Текст] / *А. А. Варфоломеев, О. С. Домнина, М. Б. Пеленицын.* – М.: МИФИ, 2006.**11.** *Березин, Б. В.* Цифровая подпись на основе традиционной криптографии [Текст] / *Б. В. Березин, П. В. Дорошкевич.* – М.: МП "Ирбис-II", 2002.**12.** Защита информации от несанкционированного доступа согласно требованиям ФСТЭК России [Електронний ресурс]. – Режим доступу: www / URL: http://www.pcweek.ru/security/article/detail.php?ID=169230 – загл. з екрану.**13.** Код Безопасности. Продукты [Електронний ресурс]. – Режим доступу: www / URL: http://www.security code.ru/products/ – загл. з екрану.**14.** Кратко о выборе сертифицированных СЗИ от НСД [Електронний ресурс]. – Режим доступу: www / URL: [http://www.altx-soft.ru/articles/show-1.htm – загл. з екрану.**15.** Автоматизация нефтегазовых предприятий на базе СУБД ЛИНТЕР [Електронний ресурс]. – Режим доступу: www / URL: https://linter.ru/ru/press-center/detail/27/1578/ – загл. з екрану.**16.** GIS 6 Secure Геодезическая информационная система [Електронний ресурс]. – Режим доступу: www / URL: http://www.shels.ru/download/gis6 secure_rus.pdf – загл. з екрану.**17.** Блочні шифри [Електронний ресурс]. – Режим доступу: www / URL: http://citforum.ru/internet/ infsecure/its2000_16.shtml – загл. з екрану.**18.** *Баричев, С. Г.* Стандарт AES. Алгоритм Rijdael [Текст] / *С. Г. Баричев, В. В. Гончаров, Р. Е. Серов.* – М.: Телеком, 2002. – С. 30–35.

Bibliography (transliterated):1. *Simmons, G. D.* (2008). Obzor metodov autentifikatsii informatsii. TIIER, 76, No 5.**2.** *Uolker, B. Dzh.* (2000). Bezopasnost' EVM i organizatsiya ikh zashchity. Moscow: Svyaz'.**3.** *Khoffman, L.* (2007). Sovremennyye metody zashchity informatsii. Moscow: «Sovetskoye radio».**4.** *Zhidkikh, A. D.* (2011). Teoreticheskiye osnovy komp'yuternoy bezopasnosti. Zhurn. «Obuchayushchaya sistema», No 1, 185–186.**5.** *Grusho, A. A., Timonina, Y. Y.* (1996). Teoreticheskiye osnovy zashchity informatsii. Moscow: Izdatel'stvo Agentstva «Yakhtsmen».**6.** *Varfolomeyev, A. A., Pelenitsyn, M. B.* (2006). Metody kriptografii i ikh primeneniye v bankovskikh tekhnologiyakh. Moscow: MIFI.**7.** *Vinokurov, A.* (2009). Kriptografiya.

Zhurn. «INFUSED BYTES».**8.** *Vinokurov, A. Y.* (2005). Yeshche raz pro GOST. Moscow: Monitor, 45.**9.** *Barichev, S.* (2008). Kriptografiya bez sekretov. Moscow: Moskva.**10.** *Varfolomeyev, A. A., Domnina, O. S., Pelenitsyn, M. B.* (2006). Upravleniye klyuchami v sistemakh kriptograficheskoy zashchity bankovskoy informatsii. Moscow.**11.** *Berezin, B. V., Doroshkevich, P. V.* (2002). Tsifrovaya podpis' na osnove traditsionnoy kriptografii. Moscow: MP "Irbis II".**12.** Zashchita informatsii ot nesanktsionirovannogo dostupa soglasno trebovaniyam FSTEK Rossii. Available at: http://www.pcweek.ru/security/article/detail.php?ID=169230 – zagl. z yekranu.**13.** Kod Bezopasnosti. Produkty. Available at: http://www.security code.ru/products/ – zagl. z yekranu.**14.** Kratko o vybore sertifitsirovannykh SZI ot NSD. Available at: http://www.altx-soft.ru/articles/show-1.htm – zagl. z yekranu.**15.** Avtomatizatsiya neftegazovykh predpriyatiy na baze SUBD LINTER. Available at: www / URL: https://linter.ru/ru/press-center/detail/27/1578/ – zagl. z yekranu.**16.** GIS 6 Secure Geodezicheskaya informatsionnaya sistema. Available at: http://www.shels.ru/download/gis6 secure_rus.pdf – zagl. z yekranu.**17.** Blochní shifri. Available at: http://citforum.ru/internet/infsecure/its2000_16.shtml – zagl. z yekranu.**18.** *Barichev, S. G., Goncharov, V. V., Serov, R. Ye.* (2002). Standart AES. Algoritm Rijdael. Moscow: Telekom, 30–35.

Поступила (received) 22.12.2015

Відомості про авторів / Сведения об авторах / About the Authors

Руженцев Віктор Ігоревич – кандидат технических наук, доцент, кафедра Безопасности информационных технологий, Харьковский национальный университет радиоэлектроники, пр. Ленина, 14, г.. Харьков, Украина, 61166; тел.: 057-702-14-25; e-mail: diagnost@kture.kharkov.ua.

Руженцев Віктор Ігоревич – кандидат технічних наук, доцент, кафедра Безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, пр. Леніна, 14, м. Харків, Україна, 61166; тел.: 057-702-14-25; e-mail: diagnost@kture.kharkov.ua.

Ruzhentsev Victor – PhD, Associate Professor, Department of Information Technology Security, Kharkov National University of Radioelectronics, Lenina Ave., 14, Kharkiv, Ukraine, 61166; tel.: 057-702-14-25; e-mail: diagnost@kture.kharkov.ua.

Порван Андрей Павлович – кандидат технических наук, старший научный сотрудник, кафедра биомедицинской инженерии, харьковский национальный университет радиоэлектроники, пр. Ленина, 14, г. Харьков, Украина, 61166; тел.: 066-294-06-70; e-mail: porvan_a_p@mail.ua.

Порван Андрій Павлович – кандидат технічних наук, старший науковий співробітник, кафедра біомедичної інженерії, Харківський національний університет радіоелектроніки, пр. Леніна, 14, м. Харків, Україна, 61166; тел.: 066-294-06-70; e-mail: porvan_a_p@mail.ua.

Porvan Andrei – PhD, Senior Research, Department of Biomedical Engineering, Kharkov National University of Radioelectronics, Lenina Ave., 14, Kharkiv, Ukraine, 61166; tel.: 066-294-06-70; e-mail: porvan_a_p@mail.ua.

Пащенко Мария Анатольевна – студентка, факультет Электронной техники, Харьковский национальный университет радиоэлектроники, пр. Ленина, 14, г. Харьков, Украина, 61166; тел.: 066-933-13-54; e-mail: maria-paschenko@mail.ru.

Пащенко Марія Анатоліївна – студентка, факультет Електронної техніки, Харківський національний університет радіоелектроніки, пр. Леніна, 14, м Харків, Україна, 61166; тел.: 066-933-13-54; e-mail: maria-paschenko@mail.ru.

Pashchenko Maria – student, Faculty of Electronic Engineering, Kharkiv National University of Radioelectronics, Lenina ave., 14, Kharkov, Ukraine, 61166; tel .: 066-933-13-54; e-mail: maria-paschenko@mail.ru.

УДК 629.33:004.056

А. В. МАКОВЕЦКИЙ

АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОВРЕМЕННОГО АВТОМОБИЛЯ

Современные автомобили представляют собой сложные технические системы, оснащенные электронными устройствами для улучшения эксплуатационно-технических свойств. Устойчивая тенденция увеличения количества электронных устройств в современных автомобилях с проводным и беспроводным подключением неизбежно приводит к росту уязвимостей, а значит – снижению безопасности и эффективности эксплуатации. Проведенный анализ позволил выявить ряд угроз информационной безопасности автоматизированных систем современных автомобилей, которые приводят к необходимости разработки методов механической и электронной защиты транспортных средств.

Ключевые слова: информация, уязвимость, защита, угроза, безопасность, эксплуатация, автомобиль.

Введение. Современные автомобили представляют собой сложные технические системы, оснащенные электронными устройствами для улучшения эксплуатационно-технических свойств. В 1990 г. электронные устройства и программное обеспечение составляли около 16 % стоимости автомобиля, в 2001 г. – 25 %, а в 2005 г. – до 40 % [1]. По оценкам специалистов Центра автомобильных исследований штата Мичиган, по состоянию на 2014 г. электроника и программное обеспечение составляют уже до 40-50 % [2] стоимости современного автомобиля. Также по данным Инженерной Ассоциации IEEE известно, что программное обеспечение представляет 90 % [3] инноваций в автомобилях.

Устойчивая тенденция увеличения количества электронных устройств в современных автомобилях с проводным и беспроводным подключением неизбежно приводит к росту уязвимостей, а значит – снижению безопасности и эффективности эксплуатации.

Анализ литературных данных и постановка проблемы. На сегодняшний день новый автомобиль содержит от 50 до 100 и более электронных блоков управления [4]. В работе [5] указывается, что к 2025 г.

©А. В. Маковецкий. 2015