**УДК 004.9**

# ОСОБЛИВОСТІ ВИКОРИСТАННЯ МЕТОДІВ ШИФРУВАННЯ В ЗАДАЧАХ ЗАХИСТУ ІНФОРМАЦІЙНИХ СОЦІАЛЬНИХ МЕРЕЖ

Б. В. Дурняк, Т. М. Хомета

*Українська академія друкарства,*
*вул. Підголоско, 19, Львів, 79020, Україна*

*Розглядаються криптографічні методи контролю доступу до складних інформаційних систем на прикладі системи контролю доступу SPX. Проведений аналіз ілюструє можливість модифікації протоколів SPX з ціллю адаптації його до потреб інформаційних соціальних систем. Така адаптація може полягати у спрощені окремих процедур цього протоколу, які обумовлюються особливостями соціальної системи.*

***Ключові слова:*** *інформаційні соціальні системи ICS, верифікація, ідентифікаційні дані, криптографія.*

**Постановка проблеми.** Задача, яка розглядається в статті, полягає у визначені можливостей модифікації відомих протоколів з ціллю адаптації їх до потреб задач захисту доступу до соціальних інформаційних систем.

**Мета статті.** Досліджується проблема контролю доступу до складних інформаційних систем, які розглядаються як захист користувача у вирішенні наступних задач: захист доступу до системи, який активізується користувачем; захист від неуповноваженого учасника процесу виконання запиту, з яким звернувся користувач до *ICS*; забезпечення безпеки персональних даних, що пов'язані з реалізацією запиту.

**Виклад основного матеріалу дослідження.** Захист доступу до системи дозволяє уникати можливості підміни користувача третьою особою. Реалізація захисту в цьому випадку може здійснюватися на основі окремої реєстрації користувача та в режимі реального часу. В першому випадку є такі можливості: особисто звернутися для реєстрації та зареєструватися дистанційно. З наведеного вище випливає, що для реалізації процесів захисту потрібна незалежна інфраструктура формування та обміну ключами формування та іншими компонентами, що необхідні для створення захищених каналів зв'язку. Одним із методів створення захищених каналів, який забезпечує високий рівень безпеки, є методика, відповідно до якої створюється система захисту доступу на основі використання протоколу *SPX* [1].

У рамках цього підходу передбачається, що користувач має доступ до хосту (*H*). В межах системи верифікується користувач на основі використання його гасла, використовуються ідентифікаційні дані користувача, час, протягом якого може бути реалізований доступ та випадкові числа, які використовуються для додаткового затінення процесів обміну, що реалізуються при ідентифікації.

Однією з особливостей соціальних систем є можливість їх інтерпретації, яка дозволяє здійснювати ілюстрацію теоретичних методів та засобів, які використовуються для розв'язання задач захисту. Така інтерпретація повинна орієнтуватися на відображення принципів, що забезпечують відповідний

захист. Крім використання механізмів захисту, для соціальних систем є актуальною можливість оцінки величини відповідного захисту, яка повинна відображати взаємозв'язок міри захищеності з мірою втрат, до яких можуть привести випадки, коли пропоновані засоби захисту не використовуються.

Наступною особливістю, характерною для соціальних систем, є необхідність визначення вартості того чи іншого рівня захищеності, який пропонується системою захисту або сукупністю певних засобів захисту. Очевидно, що міра захищеності послуг, які надаються користувачу, має певну вартість. Система захисту здебільшого реалізується таким чином, що розділяти засоби в рамках такої системи з точки зору затрат на їх реалізацію є досить важко. Це призводить до того, що послуги для клієнтів є досить коштовними. Для соціальних систем характерно надавати клієнтам послуги без оплати їхньої повної вартості. Це, в свою чергу, зумовлює необхідність використання бюджетних коштів, що не завжди є обґрунтованим чи доцільним. У зв'язку з цим необхідно багаторазові процеси обслуговування клієнтів розділити на різні категорії з точки зору потреб соціальних служб або державних органів, що такі служби організовують. Відповідні умови надання послуг, в яких зазначається тип послуги, міра захищеності даних, що пов'язані з такою послугою, кратність надання послуги певного класу та базова, або початкова кількість послуг. Тоді вартість послуги можна описати співвідношенням:

$$v = k\eta\,(r - k)\,\mu / r,$$

де $v$ – вартість послуги, $r$ – кратність виконання послуги, $k$ – тип послуги, $\eta$ – міра захищеності даних, що пов'язані з $k$, $\mu$ – міра безпеки послуги. Міра безпеки послуги буде визначатися кількістю засобів захисту, що використовуються в системі захисту соціальних систем (*CSB*), для доступу до системи надання послуги. Це означає, що $\eta$ – визначає міру захисту даних в *ICS*,а $\mu$ – визначає міру захищеності доступу до системи. Величину $v$ – можна умовно вважати вартістю послуги, яка при $r=1$ і $a=1$ де $a$ – початкова, або базова кількість послуг, рівна нулю. Очевидно, що $r \geq a$. Величина v в частині захисту доступу приймає дискретні значення. На прикладі протоколу *SPX*, зменшення $v_i$ може полягати в ігноруванні односторонніх функцій $h_1$, при формуванні посилки для локального сервера *LEAF* стороною *CDC*, що являє собою центр сертифікації і зберігає паролі всіх користувачів. У випадку зниження рівня захищеності, *CDC* можна не використовувати $h$ функції для перетворення пароля $h_1$, а замість $h_1$ може вибрати коди ряду символів для шифрування ключа $k_A$. Відповідно до цього модифікується зміст сертифіката, яким користується локальний сервер *LEAF*. Подібні модифікації можуть реалізуватися в частині протоколу аутентифікації клієнта, коли він активізує зв'язок з сервером *SPX*.

Розглянемо структурну схему реалізації аутентифікації на прикладі системи *SPX* в частині аутентифікації клієнта з сервером. Оскільки процеси, що відбуваються в окремих компонентах, складаються з цілого ряду внутрішніх операцій, а структура процесу обміну відображає взаємний обмін відповідними даними між окремими елементами, який реалізується послідовно в часі, то

в цій структурі будемо відображати процеси обміну даними, які називатимемо комунікатами, а також в цій структурі будемо відображати часову послідовність передачі відповідних даних, незважаючи на те, що це приведе до того, що елементи структури повторюватимуться.

На рис. 2.1 наведена структура процесу реалізації обміну між окремими компонентами процесу аутентифікації клієнта при його звертанні до системи.

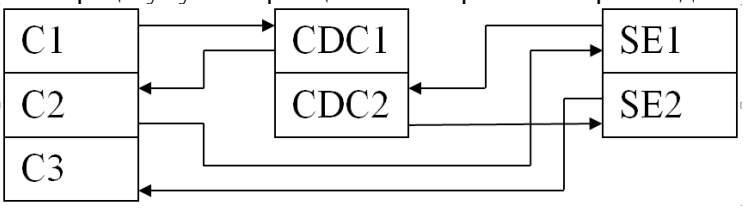


Рис. 2.1. Структурна схема взаємозв'язків між компонентами системи SPX

Цифрою, що використовується в позначеннях компонент, відображають часові залежності активізації кожної з компонент у процесі реалізації аутентифікації клієнта системою. Позначення, що використовуються на рисунку:

$C_i$ – клієнт, об'єднаний з відповідним хостом;

$CDC_i$ – сервер, що вміщає ключі шифрування;

$SE_i$ – локальний сервер ідентифікації.

Функції, які реалізуються кожною компонентою, в яких замість цифр будемо використовувати відповідні їм індекси, у виділені інтервали часу реалізації процесу аутентифікації, полягають у наступному:

– $C_1$ – клієнт, який в цьому випадку інтегрований з хостом $H$, передає до $CDC_1$ інформацію про локальний сервер у вигляді відповідного сертифіката, який клієнт отримав на етапі початкової ідентифікації, що часто називають реєстрацією клієнта. Сервер *CDC* знаходить сертифікат відкритого ключа $K_s$, що використовується для комунікацій з сервером $S$,

– $CDC_1$ – пересилає клієнту $C_2$ сертифікат, що був переданий до $CDC_1$ на попередньому циклі. Клієнт $C_2$ виконує такі дії:

1) відкриває ключ $K_s$ з сертифіката за допомогою відповідного ключа клієнта $K_c A_c$;

2) генерує свіжий ключ сесії $K$ для реалізації безпечної комунікації з сервером *SE*;

3) шифрує ключ $K_s$ з допомогою ключа сесії $K$;

4) шифрує ключ $e$ для обміну за допомогою ключа сесії $K$.

Сервер $SE_1$ — клієнт $C_2$ пересилає до сервера $SE_1$ свій ідентифікатор $C$, зашифрований ключем $K_s$, ключ сесії $K$ і білет, який складається з конкатенації сертифіката клієнта і зашифрованого ключа обміну $e$, що формально описується співвідношенням:

$$C_2 \rightarrow SE_1 : C,\ [K]_{ks},\ t_{ie}K_c = <L,C,d>K_C,\ \{e\}_k,$$

де $C$ – ідентифікатор клієнта, $[K]_{ks}$ – ключ сесії $K$, зашифрований ключем сервера *SE*, $t_{ie}K_c$ – білет, який являє собою конкатенацію сертифіката, що складається з часу актуальності надання послуги $L$ ідентифікатором клієнта $C$ та

ключ $d$ з пари ключів $(e,d)$, що використовуються в шифруванні повідомлень, які появляються в процесі взаємного обміну між клієнтом та системою, де використовується шифр *RSA*, а також цифрового підпису, в якому зашифровано ключ алгоритму *RSA*.

Сервер $SE_1$ – сервер локальної ідентифікації, на основі отриманих від клієнта даних передає до центрального сервера сертифікації ідентифікатор клієнта: $S \rightarrow CDC_2 : C$.

Сервер $CDC_2$ по ідентифікатору $C$ знаходить персональний ключ клієнта $K_c$, що використовується для обміну з системою, та передає до локального сервера $SE_2$ сертифікат, який вміщає ідентифікатор клієнта $C$ та ключ обміну $K_c$. Цей сертифікат шифрується ключем $K_c A_c$, що описується співвідношенням:

$$CDC_2 \rightarrow ES_2 : <C, K_c > K_c A_s .$$

Сервер $SE_2$ виконує такі операції: використовуючи свій приватний ключ $K_s$, відшукує ключ сесії $K$, з сертифіката дістає публічний ключ $K_c$, з сертифіката, який сервер отримав на стані $ES_1$, та являє собою $t_{ic}\ K_c = <L,C,d> K_c$, дістає $L,C,d,$ використовуючи публічний ключ $K_c$, сервер проводить перевірку ключа в $e$ і $d$ шифру *RSA*, який буде використовуватися для процедур обміну між клієнтом та системою, що полягає у наступному: для випадкового числа $a$ проводяться такі обчислення:

$$[(a^e) \equiv a] \vee [(e*d) \equiv (mod \varphi(N))],$$

де $N$ – модуль алгоритму *RSA*.

Після цього сервер $SE_2$ передає користувачу $C_3$ зашифровану сесійним ключем $K$ нову мітку часу $T+1$, що формально описується $S \rightarrow C : \{T+1\} K$. Після цього користувач може здійснювати обмін даними з системою *CS* протягом одного сеансу зв'язку.

На основі наведеного прикладу можна стверджувати, що при реалізації захисту доступу клієнта до сервера даних, необхідно організувати всі необхідні канали таким чином, щоб вони були захищені. Через розподільність системи доводиться використовувати ієрархічну систему захисту, яка складається з центру сертифікації, в якому розміщуються дані про зареєстрованих клієнтів, та локального серверу доступу, який безпосередньо обслуговує у відповідному регіоні користувача, надаючи йому необхідні сертифікати у випадку, коли користувач, виходячи з даних реєстрації, є санкціонованим клієнтом системи *ICS*. Таким чином, центр сертифікації має всі дані про клієнта, передає ці дані локальному серверу, який перевіряє, чи вони відповідають користувачу, який активізував запис. Якщо дані клієнта і центрального сервера не збігаються, то локальний сервер не дає користувачу доступу до *ICS*. Отже, навантаження по перевірці даних клієнта перекладається на локальний сервер, а центральний сервер є вільним, оскільки він обслуговує цілий ряд регіонів.

Суттєвим недоліком у такого типу системи є перекладання значної кількості процесів, що формують компоненти, орієнтовані на забезпечення захисту, наприклад, до функцій хосту належить формування випадкової величини $\tau$, яка використовується як разовий ключ у процесах реєстрації, а також вибір одно-

направлених функцій *h* для нормалізації запису ідентифікаційних даних, що являють собою пароль, та інші. Ще один недолік, який є досить загальним, полягає у надмірному використанні сертифікатів у комунікаціях центру сертифікації з локальними серверами, які, за визначенням, є найбільш захищеними. Недоліком наведеної системи ідентифікації також є те, що при вступній ідентифікації та ідентифікації клієнт-сервер існує можливість безпосереднього доступу хоста до центру сертифікації, яким в наведеному прикладі є сервер *CDC*.

Іншою властивістю соціальних систем є те, що окремі користувачі можуть мати різні профілі, або профілі, що досить суттєво відрізняються один від одного. Тому для системи типу *ICS* доцільно використовувати персональні характеристики, що сьогодні доступно, оскільки такі характеристики розміщуються в електронній формі в документах, що ідентифікують особу. Такими документами передусім є паспорти. Тому важливим аспектом методів захисту повинні бути профілі користувачів соціальної системи.

Наступною особливістю соціальних систем і, відповідно, користувачів цих систем є дані, які знаходяться у відповідній *ICS*. Одним із параметрів, що характеризують ці дані, є те, що вони переважно є досить стабільними. Це означає, що міра незмінності цих даних для кожного окремого клієнта і, відповідно, міра їх специфіки може використовуватися для розпізнавання для неуповноваженого користувача. Для цього застосовуються методи, що ґрунтуються на використанні профілів порушень, або аномалій, які прийнято називати інтрузами. Ці методи досить широко використовуються в системах *IDS* (Intrur Detection System) [2, 3].

Розглянемо параметр, який характеризує незмінність даних окремого користувача. Приймемо, що впроваджувати зміни в ці дані може, насамперед користувач. В окремих системах вводити дані, які стосуються користувача, можуть треті особи, але це робиться з відома користувача, наприклад, у випадку інформаційних медичних систем, що зберігають дані про захворювання, які вносяться в систему, коли користувач звертається до лікарів.

Досить поширені методи виявлення аномалій доступу ґрунтуються на різних методах, що використовують засоби теорії ймовірності [4]. Досить розвинутим є підхід, що ґрунтується на теоремі Байєса [5]. Одного співвідношення Байєса недостатньо, щоб можна було його використовувати для виявлення інтрузів на основі аналізу подій, що мають місце в інформаційному середовищі. Розширення теоретичних можливостей полягає у введені додаткових функцій оцінок, якими є уявлення про позитивні та негативні відхилення від справедливості гіпотези про наявність інтруза, які описуються співвідношеннями:

$$O(I) = \frac{P(I)}{P(\tilde{I})} \text{ та } O(I/e) = \frac{P(I/e)}{P(\tilde{I}/e)},\ O(I) > \frac{P(I)}{P(\tilde{I})}.$$

Ці співвідношення $P(\tilde{I})$ характеризують еволюційну істинність гіпотези про те, що в системі появився інтруз. З наведених співвідношень видно, що позитивне відхилення того, що появився інтруз *O(I)* дорівнює відношенню

відповідних ймовірностей. Крім того, вводяться уявлення про позитивну та негативну подібність, що описується співвідношенням:

$$S\left(e/I\right)=\frac{P\left(e/I\right)}{P\left(e/\tilde{I}\right)} \quad \text{та} \quad N\left(e/I\right)=\frac{P\left(\tilde{e}/I\right)}{P\left(\tilde{e}/\tilde{I}\right)}.$$

Позитивна подібність характеризує подію *e* щодо її зв'язку з подією негативною, якщо *S(e/I)>1*, то подія *e* підтверджує гіпотезу *I*. Розвитком цього підходу є теорія Депстера [6]. У цій теорії вводиться функція вірогідності, що формально описується наступним співвідношенням:

$$Bel(\omega)=\sum a\subseteq\omega m(a),$$

де – $\omega\subseteq\Omega$ – міра правдоподібності того, що дана підмножина подій $\omega\epsilon r^{\Omega}$, показує ймовірність всіх подій a, що залежать від $\omega(\omega\cap a\neq\emptyset)$. Функція *Bel(ω)* визначає нижню границю довіри до *m*, а функція *Pl(ω)* – верхню границю довіри до $\omega$. Можна записати, що $P\left(\omega\right)=1-Bel\left(\overline{\omega}\right)$, де $\overline{\omega}$ – альтернативна подія по відношенню до події $\omega$.

Основним результатом цієї теорії є правило комбінації Депстера, що полягає у наступному. Нехай $\Omega$ є множиною елементарних подій $am_1,m_2$, є дві базові припорядковані ймовірності. Комбінованим припорядкуванням ймовірності називається функція $m_1\otimes m_2:r^{\Omega}\rightarrow(0,1)$, що визначається залежністю

$$m_1\otimes m_2(\omega)=\frac{\sum a\cap\beta=\omega m_1(a)m_2(\beta)}{\sum a\cap\beta\neq\phi m_1(a)m_2(\beta)}$$

для всіх $\omega\neq\emptyset$. Це правило дозволяє вимірювати всі обґрунтовування «за» і «проти» гіпотези. Це вимірювання реалізується на основі конструювання комбінованих припорядкованих ймовірностей на основі двох обґрунтувань, що випливають з експериментальних даних.

В загальному функція $Bel\left(\overline{\omega}\right)$ є мірою величини обґрунтувань, що протидіють прийнятій гіпотезі $\omega$, а функція *Bel(ω)* є мірою величини сприяння гіпотезі $\omega$. Розглянемо деякі окремі випадки, що визначаються різними значеннями окремих введених функцій.

Приймемо, що *Pl(ω)-Bel(ω)=1*. Це означає, що *Pl(ω)=1* та *Bel(ω)=0*. Це, своєю чергою, означає, що всі події, для яких $\omega$ є надмножиною, ніколи не виникають, а для всіх інших подій $\omega$ є відповідною, або правильною підмножиною. Тоді кожне поодиноке спостереження вміщає $\omega$ як константу. В цьому випадку не має підстав суперечити гіпотезі $\omega$. У випадку, коли *Pl(ω)=0* з чого випливає *Bel(ω)=0*, будь-яка подія має не пусту частину, спільну з $\omega$, і ніколи не відбувається. Тому гіпотеза ω є фальшивою.

Коли *Bel(ω)=1*, що приводить до того, що *Pl(ω)=1*, то кожна подія повинна бути підмножиною $\omega$. В цьому випадку гіпотеза ω є правдивою.

Коли $Pl(\omega)=\varepsilon_1$ та $Bel(\omega)=\varepsilon_2$ і $\varepsilon_1>\varepsilon_2$ та $\varepsilon_1,\varepsilon_2=<0,1>$, то існують аргументи, або обґрунтування, які, як і заперечують гіпотезу $\omega\left(Bel\left(\varpi\right)=1-\varepsilon_1\right)$, і підтверджують її правильність $(Bel(\omega)=\varepsilon_2)$.

Розширення цього підходу полягає у використанні множини експериментальних даних про те, що подія $\omega$ відбулась, що відповідає гіпотезі *I*, та

даних про всі випадки виникнення подій, які не відповідають гіпотезі *I* або $\tilde{I}$. При проведені аналізу цих подій можна говорити про існування деякого розподілу ймовірності виникнення подій, які відповідають гіпотезі *I*, що формально можна записати у вигляді:

$$P(\omega)=F(\omega,x),$$

де $\omega$ – подія, ймовірність якої нас цікавить, а $x$ – змінна, що визначає параметр, по відношенню до якого визначається зміна ймовірності $P(\omega)$. Прикладом такого параметра може бути час, протягом якого проводяться експерименти. Якщо б закон розподілу $F(\omega,x)$ на всіх інтервалах часу залишався постійним, то, при виявленні інтрузів, не виникало би проблем. Але на практиці закони розподілу з часом міняються і, відповідно міняються функції, по яких можна обчислити відповідні ймовірності. В цьому випадку існують наступні можливості вирішення цієї проблеми.

Перша можливість ґрунтується на встановленні функції, що описує ймовірність зміни $F(\omega,x)$ залежно від переходу з одного інтервалу $\Delta t_i$ до інтервалу $\Delta t_{(i+1)}$. Приймемо, що зміна функції $F(\omega,x)$ буде залежати ще від параметра $t$, або буде мати місце $F(\omega,x,t)$. Для більш конструктивного розгляду цього підходу необхідно перейти до функції розподілу, що найбільшою мірою, з точки зору її інтерпретації, відповідала би поставленій задачі. Тому уточнимо умови задачі, яку будемо розглядати. В даному випадку подіями, що розглядаються, є рідкісні події, оскільки приймається, що вторгнення інтруза в систему не має регулярного характеру і відбувається послідовно в часі у випадкові моменти процесу функціонування системи. В певній мірі можна прийняти такий випадковий процес як процес з хаотичним розподілом у часі. Відповідно до відомого твердження [7], Пуасоновський точковий процес можна розглядати як модель абсолютно хаотичного розподілу подій в часі. Формально відповідна теорема приводить до наступного виразу для ймовірності виникнення відповідних подій:

$$P(\varepsilon_j\in[\tau_j,\tau_j=h]),j=1,\ldots,n|\varepsilon|(b\text{-}\varepsilon(a)=n)=\frac{n!}{(b-a)^n}h^n,$$

де $[a,b]$ – інтервал, на якому розглядаються події пуасоновського процесу з інтенсивністю $\lambda>0,\tau_j$, для $j>0$ це означає подію, що відбувається на інтервалі $[a,b],n$ – загальна кількість подій $\tau_j$ на інтервалі $[a,b],h$ – величина інтервалу між подіями, де $h>0$, але настільки мале, що $h<\underbrace{\min}_{o\le j\le n}(t_{j+1}-t_j)$. Для формування інтерпретації цього підходу до опису процесів виникнення інтрузів, необхідно розглянути інформаційні властивості вибраного підходу. Згідно з визначенням кількості інформації за Шеноном, інформацією, що вміщається в події *B* по відношенню до події *A*, називається величина, що визначається співвідношенням:

$$I(AIB)=\log[P(AIB)/PA].$$

Якщо $B=A$,то $I(AIA)=-\log P(A)$ *і тоді* $I(A)=-\log P(A)$. Для того щоб показати, що розподіл, про який йдеться, має властивість невизначеності, необхідно розглянути загальну модель невизначеності. Відомо, що поняття невизначеності пов'язане з поняттям інформації. Приймемо, що експеримент

$\varepsilon$, може привести до одного з результатів $A_1, A_2, ..., A_n$. Тоді $P(A_i)=P_i$, інформацію, отриману в результаті цього експерименту, можна вважати випадковою величиною, що приймає значення $I(A_1), ..., I(A_n)$ з ймовірностями $P_1, ..., P_n$. На основі цих припущень вводиться інформаційна характеристика, що називається ентропією [5]. Ентропія $H(\varepsilon)$ експерименту є визначається величиною:

$$H(\varepsilon)=EQ(\varepsilon)= -\sum^{n}_{(i=1)} P_i \log P_i,$$

де $Q(\varepsilon)$ – випадкова величина, що визначає міру визначеності отримання результату експерименту. В такій інтерпретації ентропія є мірою невизначеності.

Відповідно до твердження про властивості ентропії, для послідовності випадкових подій, які розглядаємо як результат послідовності випадкових експериментів, можна записати співвідношення:

$$H(x_\delta)=\sum^{n}_{(i=1)} P(x_i^*)\delta \log P(x_i^*) - \log\delta,$$

де перший складник являє собою інтегральну суму Дарбу для величини $H(x)$. Тому можна записати:

$$H(x)=lim_{\delta\to 0} |H(x_\delta)+\log\delta|,$$

де $\delta$ – довжина інтервалу в області значень $x$, $x_i^* \in \Delta$, де $\Delta$ – інтервал, в який попадає значення $x_i^*$, $x_\delta$ – дискретна апроксимація величини $x$ така, що $x_\delta \to x$, при $\delta \to 0$. Величину $\log\delta$ можна інтерпретувати як інформацію, що вміщається в події, ймовірність якої рівна $\delta$. Тому можна вважати, що $H(x)$ характеризує невизначеність неперервної величини $H(x)$, а саме ця величина називається диференціальною ентропією випадкової величини $x$. Згідно з відомим твердженням, пуасоновський процес є найбільш невизначеним, найбільш хаотичним процесом серед усіх процесів відновлювання, зі скінченним математичним сподіванням, з неперервним розподілом віддалей для $\xi_j$, $j>1$.

**Висновки.** У статті проаналізовано особливості використання криптографічних методів захисту в задачах інформаційних соціальних системах. Завдяки аналізу таких особливостей вдалося сформулювати окремі задачі захисту інформації, які насамперед стосуються захисту доступу до неї.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Тардо Ж., Алладжепен К. СПХ : Глобальная аутентификация и использование общественных ключевых свидетельств. В.: Продолжение 12-го Симпозиума об Исследованиях в области безопасности и конфиденциальности. — 1991. — С. 261–268.
2. Аморозо Е. Проявление Интрузии / Е. Аморозо. — Варшава : PM, 1999.
3. Столлинг В. Основы защиты сетей. Приложения и стандарты / В. Столлинг. — К. : ВХБб, 2000.
4. Бендат Дж. Прикладной анализ случайных данных / Дж. Бендат, А. Пирсон. — М. : Мир, 1989.
5. Яглом А. М. Вероятность и информация / А. М. Яглом, И. М. Яглом. — М. : Наука, 1973.
6. Депстер А. Генерализация Баезианских выводов. Журнал Королевского Статистического Общества, 30: 205–247, 1968.
7. Королёв В. Ю. Теория вероятностей и математическая статистика / В. Ю. Королёв. — М. : Проспект, 2005.

**REFERENCES**

1. Tardo, Zh., & Alladzhepen, K. (1991). SPKh: Globalnaia autentifikatsiia i ispolzovanie obshchestvennykh kliuchevykh svidetelstv. V.: *Prodolzhenie 12-ho Simpoziuma ob Issledovaniiakh v oblasti bezopasnosti i konfidentsialnosti*, (pp. 261–268) [in Russian].
2. Amorozo, E. (1999). *Proiavlenie Intruzii* [*Wykrywanie Intruzow*]. Warshawa: RM [in Polish] .
3. Stolling, V. (2000). *Osnovy zashchity setei. Prilozheniia i standarty*. Kiev : VKhBb [in Russian].
4. Bendat, J., & Pirson, A. (1989). *Prikladnoi analiz sluchainykh dannykh*. M. : Mir [in Russian].
5. Yaglom, A. M., & Yaglom, I. M. (1973). *Veroiatnost i informatsiia*. M.: Nauka [in Russian].
6. Depster, A. (1968). *Generalizatsiia Baezianskikh vyvodov*. Zhurnal Korolevskogo Statisticheskoho Obshchestva, 30, 205-247.
7. Korolev, V. Yu. (2005). *Teoriia veroiatnostei i matematicheskaia statistika* M.: Prospekt [in Russian].

## PECULIARITIES OF ENCIPHERING METHODS FOR INFORMATIVE SOCIAL NETWORKS PROTECTION

B. V. Durniak, T. M. Khometa

*Ukrainian Academy of Printing,*
*19, Pidholosko St., Lviv, 79020, Ukraine*
*taraskhometa@gmail.com*

*Cryptographic methods of access control to complex informative systems using the SPX access control system are under consideration. Performed analysis shows the possibility of SPX protocols modification with the purpose of their adaptation to the requirement of informative social systems. Such adaptation may imply simplification of certain procedures of this protocol stipulated by peculiarities of the social system.*

***Keywords:*** *informative social systems ICS, verification, identification data, cryptography.*

*Стаття надійшла до редакції 15.04.2015.*
*Received 15.04.2015.*