ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ НЕОДНОЗНАЧНОГО ШИФРОВАНИЯ

Гальченко А. В.

Запорожский национальный университет,
ул. Жуковского, 66, г. Запорожье, 69600

andrem1993@ukr.net

В данной статье рассматривается проблема защиты персональных данных, которая является весьма актуальной в современном мире. Эта проблема освещается и различными государственными службами, которые занимаются вопросами безопасности, в средствах массовой информации и специалистами в области информационной безопасности. В данной статье рассмотрена проблема использования традиционных и современных средств защиты информации в информационных системах персональных данных (далее – ИСПДн). Автором статьи освещается идея использования средств неоднозначного шифрования данных для защиты информации в ИСПДн. В ходе работы автор исследовал проблемы защиты персональных данных, сделал обзор литературы и ресурсов в сети Интернет, на которых описаны традиционные и современные механизмы их защиты, а также выполнил обзор литературы, анализ алгоритмов неоднозначного шифрования, выбрал среди них наиболее адаптированный для выполнения поставленной задачи и сравнил его эффективность с традиционными и современными подходами к защите информации в ИСПДн. Для наведения практических результатов автор выполняет шифрование/дешифрование тестовой ИСПДн с использованием традиционных, современных и неоднозначных средств шифрования данных.

Ключевые слова: персональные данные, информационная система, деперсонализация данных, шифрование, отрицаемое шифрование, грубая сила, перемешивание данных, bigdata.

PROTECTION OF PERSONAL DATA WITH USE ALGORITHMS OF NON-DIGITAL SHIFT

Galchenko A. V.

Zaporizhzhya National University,
Zhukovsky str., 66, Zaporizhzhya, 69600, Ukraine

andrem1993@ukr.net

The article deals with the problem of protection of personal data, which is very relevant in the modern world. This problem is covered in the media by various state security services and information security specialists. This article breaks down the problem of using traditional and modern means of protecting information in information systems of personal data (hereinafter - ISPD). The author of the article describes the idea of using the means of deniable data encryption to protect information in the ISPD. In the course of the research, the author studied the problem of personal data protection, made a review of literature and resources on the Internet, which described the traditional and modern mechanisms for their protection, and also conducted a review of literature, analysis of deniable encryption algorithms, selected among them the most adapted to fulfill the task and compared its effectiveness with traditional and modern approaches to protecting information in the ISPD. To provide practical results, the author encrypts / decrypts the test ISPDs using traditional, modern, and deniable data encryption tools. The described researches were carried out by the postgraduate student of the department of software engineering of Zaporizhzhya National University in the framework of the dissertation research «Investigation of instrumental mechanisms of denied encryption».

Prior to conducting the above studies, the following objectives were set: substantiation of the need to protect personal data in the modern information space; an overview of traditional and modern means of information protection in the ISPD; presentation of possibilities of deniable encryption for information protection in ISSPD; substantiation of advantages of the use of means of deniable encryption in comparison with traditional and modern means of information protection in ISPD; giving practical examples of the use of traditional, modern means and means of deniable encryption on the example of a small (theoretical) ISPD; justification for the need to further explore the possibility of using deniable encryption tools.

The novelty of this is that the issue of using deniable encryption tools has not become widespread and practical because of the unlawfulness of the methods of protection that are implemented in them. Thus, the possibilities of its use in various fields of data processing such as protection of personal data, the formation of electronic digital signatures, etc. were not considered before.

As a result of these studies, the following results were obtained: review of traditional and modern encryption tools, as well as presentation of possibilities of deniable encryption tools for protection of information in the ISDF; the necessity of protecting personal data in the modern information space, the advantages of using the means of deniable encryption in front of traditional and modern means of information protection in the ISND is substantiated; practical examples of the use of traditional (on an example of the RSA algorithm), modern means (on the example of the algorithm of personalization depersonalization of personal data) and means of deniable encryption (on the example of the deniable algorithm on the basis of extended cryptographic scheme of Rabin) using arbitrary (test) ISPDs are presented.

Key words: personal data, information system, depersonalization, encryption, deniable encryption, coercion, operator, mixing data, bigdata.

ПОСТАНОВКА ПРОБЛЕМИ

Одним із основних векторів атак на інформаційні системи в сучасному інформаційному просторі є отримання персональних даних (далі – ПДн) про користувачів цих систем і їх оточення. Загалом до ПДн відносяться відомості чи сукупність відомостей про фізичну особу, за допомогою яких вона ідентифікується або може бути однозначно ідентифікована. Такими даними є прізвище, ім’я, ім’я по батькові, дата народження, місце проживання, телефон тощо [1].

Однак у 21 столітті наведений перелік ПДн зазнав суттєвих змін. Через стрімкий розвиток інформаційних технологій, комп’ютеризація проникла майже до усіх ключових для життєдіяльності людини галузей інфраструктури. Унаслідок переміщення діяльності людини до електронного інформаційного простору наведений вище перелік ПДн можна розширити, додавши:

– облікові дані користувачів для доступу до електронної пошти, соціальних мереж і інших інформаційних ресурсів у мережі Інтернет;

– номери кредитних карток, які використовуються для здійснення покупок, оплати праці та різноманітних послуг;

– дані про звички, вподобання та відмітки про місцезнаходження особи;

– фото та відео матеріали, які особа публікує в мережі Інтернет;

– дані про інформаційні ресурси, які відвідує особа.

Указані дані з’являються та оновлюються в мережі щодня. Їх систематичний збір та аналіз дозволяє більш точно здійснити ідентифікацію особи та галузей її діяльності, аніж традиційний перелік ПДн. Додатковий перелік даних дозволяє будь-кому вести спостереження за особою через мережу Інтернет, без використання спеціалізованих засобів знімання та збору інформації.

Значне використання ПДн у мережі, а також їх досить умовний захист, значно полегшує завдання для зловмисників зі збору та аналізу інформації, при підготовці координованих кібератак на об’єкти інформаційної діяльності. У зв’язку з цим безпека ПДн, як одного з вектору кібератак, стає все більш актуальним питанням у галузі інформаційної безпеки.

Для захисту ПДн розроблено безліч заходів [1-3]:

– організаційних (наприклад, створення законів про порядок обробки і захисту ПДн [2], розробка методик і політик з використання та захисту ПДн [1], при роботі з інформаційними системами тощо);

– технічних (наприклад, резервне копіювання та відновлення даних, контроль цілісності та доступу до обладнання інформаційних систем обробки персональних даних (далі – ІСПДн тощо) [3];

– програмних (наприклад, програмні засоби з контролю доступу до даних і їх використання, шифрування даних, деперсоналізація даних [3] тощо).

Проте, в умовах розвитку сучасного інформаційного простору, вказані вище методи захисту втрачають свою ефективність [4].

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблема захисту ПДн є одним із основних векторів атак на об'єкти інформаційної діяльності (далі – ОІД). Для їх захисту використовуються різноманітні засоби. Але через щоденне використання ПДн людиною для вирішення багатьох задач, від вибору продуктів на сніданок до придбання нерухомості, їх захист є досить складною справою.

Мало не кожний інформаційний ресурс у мережі Інтернет (далі – ІР), під приводом покращення сервісів і надання послуг, вимагає від особи надати деяку кількість ПДн, в електронному чи сканованому вигляді. Інші ж взагалі відмовляються надавати будь-які послуги без отримання від особи ПДн і згоди на їх обробку. Отже, поширення ПДн у мережі та на різноманітних носіях інформації стає все більш неконтрольованим з боку особи-власника ПДн.

З огляду на стан проблеми сьогодні [4], для вирішення вказаних вище проблем вже використовуються такі засоби захисту [1-3]:

– шифрування даних;

– використання двофакторної автентифікації (для доступу до ІР);

– використання засобів анонімізації (для приховання присутності користувачів на певних ІР);

– часті зміни ключів доступу до даних (для виключення можливості їх підбору);

– покращення криптостійкості ключів (дотримання вимог до формування та використання ключів на ІР);

– розмежування доступу до ПДн (для обмеження доступу до ПДн).

Усі описані вище засоби захисту є безперечно важливими і ефективними. Але їх застосування в сучасних умовах безпеки інформаційного простору, у зв'язку з відсутністю стандартизації засобів безпеки ІР та неможливістю синхронного усунення виявлених у них вразливостей, ускладнює забезпечення усесторонньої безпеки ПДн, які обробляються ними.

Відносно новим, порівняно з указаними вище способами захисту ПДн, є деперсоналізація ПДн. Дослідження у цьому напрямі проводяться в останні роки [5-9] і набувають усе більшої актуальності серед фахівців з інформаційної безпеки. Новий підхід до захисту даних дозволяє забезпечити додатковий рівень захисту, не виходячи за межі обмежень, встановлених діючим законодавством України. Але їх практичне застосування ускладнене через деякі технічні та організаційні тонкощі реалізації, про що свідчить їх незначне застосування для захисту ІСПДн [5-9].

Крім того, власне, особа-власник ПДн не завжди розуміє небезпеку безконтрольного поширення своїх ПДн та є необізнаною в питанні їх захисту [1, 4].

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ

Головною проблемою захисту ПДн є неможливість перешкоджання їх безконтрольного поширення як на матеріальних носіях інформації, так і в мережі. Традиційні засоби забезпечення їх конфіденційності передбачають лише розмежування доступу до ІСПДн і використання шифрування даних.

Проте ПДн, на відміну від тимчасових даних, потребують більш тривалого зберігання. Тому на системи захисту ІСПДн накладаються додаткові обмеження (наприклад, розмір ключів шифрування, частота їх зміни, додаткові механізми контролю доступу до ІСПДн).

Окрім того, є безліч проблем, пов'язаних з генеруванням і зберіганням вказаних ключів шифрування даних. Зокрема:

– необхідність використання надійних генераторів ПСП;

– використання додаткових маніпуляцій з ключами для збільшення їх стійкості до зламу (наприклад, обчислення хеш-образу, розширення або поділ ключа).

Для обходу усіх цих механізмів захисту розроблено безліч моделей і програмного забезпечення, які дозволяють імітувати їх роботу та знайти вразливості в них [10]. Але жодний із зазначених механізмів захисту не забезпечує захист від найпростішої атаки шляхом застосування примушування до операторів криптографічних систем, а також використання порушень ними правил із використання ключів.

В основі вказаних вразливостей лежить людський фактор, який жодна система захисту не може передбачити. Звісно, існують складні системи захисту, в основі яких лежить використання нейронних мереж і систем зі штучним інтелектом. Але вартість таких систем пропорційна їх складності, а їх обслуговування потребує особливих навичок від технічного персоналу та фахівців з інформаційної безпеки. Подібним і більш економічним рішенням є винайдення нових підходів до захисту інформації з використанням існуючих механізмів безпеки. Прикладом такого рішення є використання алгоритмів неоднозначного шифрування даних.

ПОСТАНОВКА ЗАВДАННЯ

Для визначення можливості використання неоднозначного шифрування даних в ІСПДн необхідно:

– сформувати узагальнену модель ІСПДн і підсистеми шифрування даних;

– виконати аналіз використання традиційних методів шифрування даних, згідно з загальною моделлю;

– внести необхідні зміни в узагальнену модель традиційного захисту даних, які б ураховували можливість використання алгоритмів неоднозначного шифрування;

– перевірити можливість і оцінити ефективність застосування методів неоднозначного шифрування на ряду з традиційними системами шифрування;

– на основі проведених перевірок сформувати рекомендації щодо можливості застосування методів неоднозначного шифрування для захисту інформації в ІСПДн.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Загалом, згідно з [1], будь-яку ІСПДн можливо представити у вигляді схеми (рис. 1).

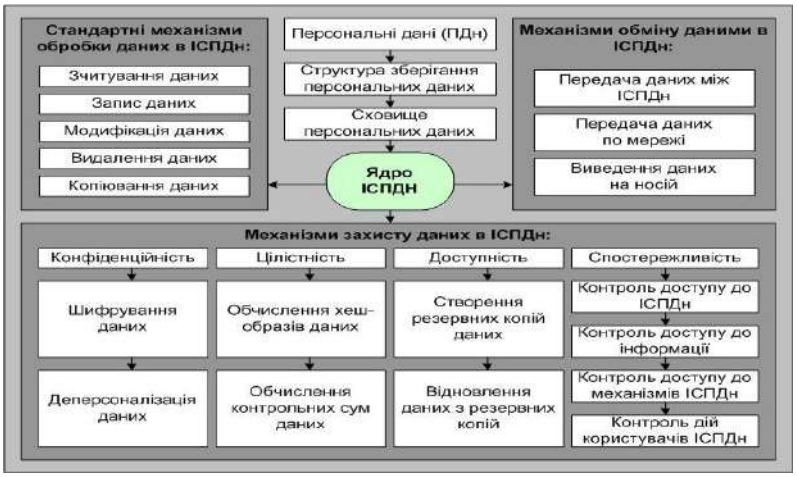

Рис. 1. Загальна схема ІСПДн

Згідно з вище наведеною схемою для забезпечення конфіденційності інформації в ІСПДн переважно використовуються лише механізми шифрування та, як один із нових напрямів, деперсоналізації ПДн.

Механізми шифрування даних в ІСПДн реалізують перетворення відкритих ПДн у нечитабельний вигляд, які забезпечують їх захист від компрометації сторонніми особами. Загалом усі перетворення підсистеми шифрування побудовані на базі симетричних криптографічних систем шифрування даних і передбачають їх довготривале зберігання. Але для обміну даними між іншими ІСПДн та в мережі використовуються асиметричні криптографічні системи шифрування даних. Здебільшого усі механізми шифрування реалізовані у вигляді окремих спеціалізованих бібліотек і мережевих протоколів, з відкритим вихідним кодом (тобто доступні для аналізу будь-кому), які реалізують набір перетворень $F(x)$. Тобто, у випадку обходу зловмисниками підсистеми контролю доступу до ІСПДн, підсистема шифрування даних дозволяє захистити їх від компрометації та крадіжки. Усі механізми шифрування побудовані на основі подібних схем перетворень інформації, повний цикл перетворень яких можна описати схемою на рис. 2.

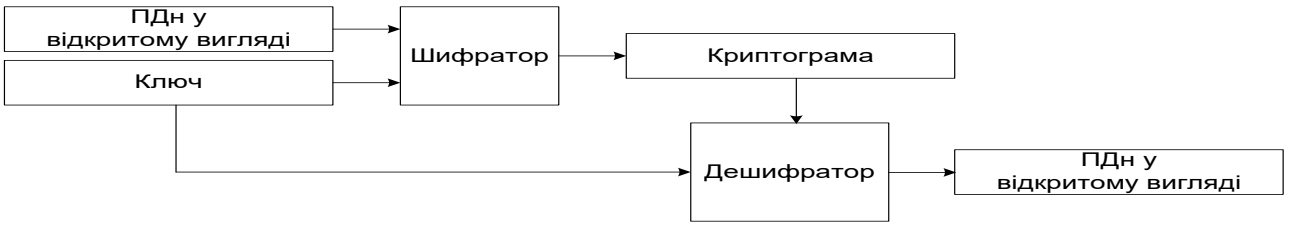

Рис. 2. Схема повного циклу перетворень інформації підсистемою шифрування даних в ІСПДн

Приклад 1: виконаємо захист вихідного значення ПДн за допомогою алгоритму RSA. Нехай вихідне повідомлення $M = 65$*, ключі згенеровані за алгоритмом RSA* $(e, d, N) = (7,343,527)$*. Тоді в результаті шифрування повідомлення отримаємо криптограму* $C = M^e \pmod N = 65^7 \pmod{527} = 482$*, а при дешифруванні отримаємо вихідне повідомлення* $M' = C^d \pmod N = 482^{343} \pmod{527} = 65$.

Для отримання вихідного повідомлення M з криптограми C зловмисникові необхідно виконати факторизацію модуля N і обчислення секретного ключа (d, N). Зі значенням $N = 527$ ця задача є досить простою, тобто $t \to 0$. Але при використанні, наприклад, n-бітних ключів ця задача стає досить складною для вирішення за короткий час, тобто $t \to \infty$.

Хоча задача на факторизацію великих чисел досить складна для вирішення та потребує великих обчислювальних потужностей і часу, але при використанні паралельних обчислень та об'єднання потужностей n-комп'ютерів стає можливою для вирішення за досить прийнятний час (чим більше комп'ютерів поєднано для проведення обчислень, тим менший час їх виконання). Тому надійність таких підсистем захисту втрачає актуальність, особливо останнім часом [4, 10].

З іншого боку механізми деперсоналізації інформації не передбачають складних математичних перетворень вихідних ПДн. В основі роботи підсистеми деперсоналізації даних лежить перемішування даних ІСПДн, у відкритому вигляді, згідно з певним алгоритмом або закономірністю. Такий підхід зручно реалізовувати через те, що в основі усіх баз даних лежить використання табличних структур зберігання даних (рис. 3):

Ідентифікатори / Атрибути	*Атрибут 1*	*Атрибут 2*	...	*Атрибут N*
Ідентифікатор 1	a11	a12	...	a1N
Ідентифікатор 2	a21	a22	...	a2N
...	...	...	...	...
Ідентифікатор M	aM1	aM2	...	aMN

$\xrightarrow{F(x,y)}$

Ідентифікатори / Атрибути	*Атрибут 1*	*Атрибут 2*	...	*Атрибут N*
Ідентифікатор 1	a21	aMN	...	a1N
Ідентифікатор 2	a13	aM2	...	aM1
...	...	...	...	...
Ідентифікатор M	a2N	a13	...	a12

Рис. 3. Загальна схема реалізації деперсоналізації даних в ІСПДн

Приклад 2: виконаємо примітивну деперсоналізацію таблиці з ПДн за допомогою простого алгоритму перемішування даних. Нехай таблиця A містить вихідні значення ПДн, а таблиці π і π^{-1} закони переміщення даних у вихідній таблиці A:

$$A=\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}\quad \pi=\begin{pmatrix}(3,3)&(2,1)&(2,3)\\(1,1)&(3,2)&(1,2)\\(2,2)&(1,3)&(3,1)\end{pmatrix}\quad \pi^{-1}=\begin{pmatrix}(2,1)&(2,3)&(3,2)\\(1,2)&(3,1)&(1,3)\\(3,3)&(2,2)&(1,1)\end{pmatrix}.$$

Тоді в результаті деперсоналізації даних у таблиці A отримано таблицю C, а при виконанні зворотних перетворень отримаємо вихідну таблицю A':

$$C=\pi(A)=\begin{pmatrix}9&4&6\\1&8&3\\5&3&7\end{pmatrix}\quad A'=\pi(C)=\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}.$$

Для отримання вихідної таблиці з відкритими ПДн зловмисникові необхідно отримати доступ до таблиці зворотних перетворень π^{-1} або виконати підбір $(M\cdot N)!$ комбінацій, з використанням деперсоналізованих ПДн. Окрім того, виконавши аналіз перетворень π, зловмисник може зрозуміти зворотній алгоритм переміщення даних і тим самим отримати вихідну таблицю з ПДн.

Отже, усі описані вище перетворення можна узагальнити схемою (рис. 4), згідно з якою в обох випадках існують схеми зворотних перетворень, при отриманні ключових параметрів яких зловмисник може отримати ПДн у відкритому вигляді без отримання відповідного на те доступу.

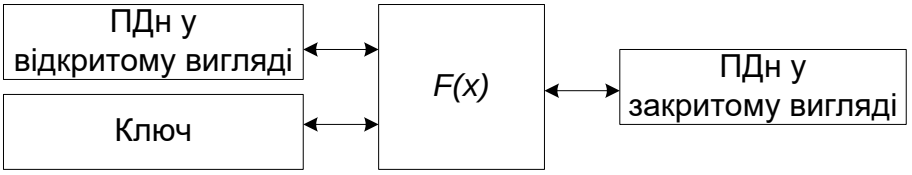

Рис. 4. Узагальнена схема перетворень ПДн в ІСПДн

За результатами аналізу вказаних вище підсистем захисту ІСПДн (шифрування та деперсоналізація даних), у процесі забезпечення конфіденційності даних в ІСПДн, отримано інформацію про їх переваги та недоліки (табл. 1).

Таблиця 1 – Результати аналізу підсистем захисту ІСПДн

Параметри аналізу	Підсистеми захисту	
	Шифрування	Деперсоналізація
Сімейство алгоритму	Симетричні, асиметричні	Симетричні
Схема перетворень	Підстановка, перестановка, розширення ключа, використання виразу $a^x(\mathrm{mod}\,n)$, циклічні перетворення	Підстановка, перестановка
Наявність ключів шифрування	Так	Так
Стійкість ключів до компрометації	Ні	Ні
Стійкість до підробки ключів	Так	Ні

Продовження табл. 1

Параметри аналізу	Підсистеми захисту	
	Шифрування	Деперсоналізація
Стійкість до підбору ключів	Так	Так
Обчислювальна стійкість	Так	Ні
Стійкість до застосування примусу	Ні	Ні
Стійкість до атак на основі відкритих ПДн	Так	Так/Ні
Стійкість до атак на основі шифрованих ПДн	Так	Так/Ні
Стійкість до атак на основі реверс інжинірингу алгоритму	Так	Так/Ні
Стійкість до атак MITM	Ні	Так

Згідно з наведеними вище даними, основними вразливостями перевірених підсистем є:

– неможливість забезпечення належного зберігання ключів (виникає внаслідок дії людського фактору, але може бути усунуте шляхом використання апаратних ключів і застосування фізичних методів захисту до них);

– нестійкість підсистем до атак із застосуванням примушування до абонента ІСПДн з боку зловмисників (виникає внаслідок дії людського фактору та не може бути усунута шляхом використання технічних, організаційних або програмних заходів захисту ІСПДн).

Указані вище проблеми є наслідком того, що будь-яка інформація має свою ціну, а в разі застосування до неї засобів шифрування її цінність може стати ще більшою. Отже, з урахуванням зазначених вище проблем узагальнена схема (рис. 4) зазнає певних змін (рис. 5).

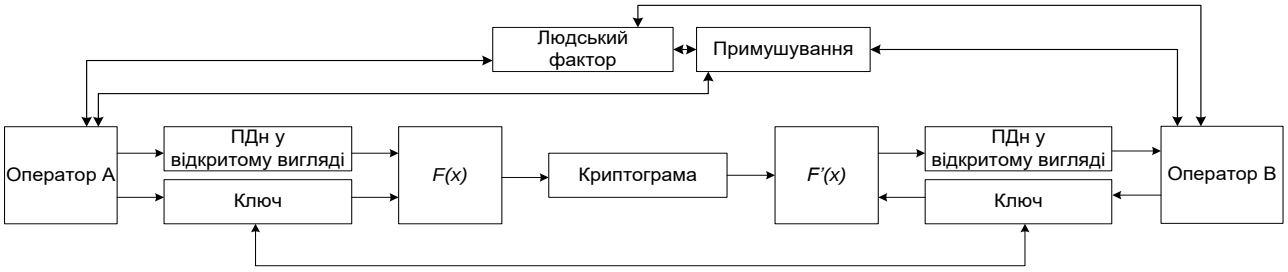

Рис. 5. Узагальнена схема перетворень ПДн в ІСПДн (з урахуванням проблем людського фактору та примушування)

Традиційно вирішення вказаних вище проблем здійснюється при застосуванні організаційних засобів захисту. Проте, як було вказано вище, у випадку впливу людського фактору на роботу підсистем захисту, їх надійність не може бути гарантованою. Тому для вирішення вказаних вище проблем необхідно застосовувати підхід із неоднозначним шифруванням даних, який дозволяє заперечити сам факт їх існування в ІСПДн або підробити їх значення, з метою захисту останніх.

На тему неоднозначного шифрування створено декілька праць [11-16] і програмних засобів [15, 16], які демонструють їх роботу, але вони не отримали широкого застосування через свій теоретичний характер, складність технічної реалізації і обґрунтування законності їх застосування. Оскільки їх надійність ґрунтується на обчислювальній стійкості діючих криптографічних систем шифрування даних, і якщо останні можна зламати з використанням/без використання ключів, то алгоритми неоднозначного шифрування не піддаються зламу (з використанням загально прийнятих методів), оскільки усі дані носять

псевдовипадковий характер. Тобто, без знання тонкощів реалізації алгоритму і ключів шифрування, їх злам ускладнюється в кілька разів. Найбільш відомими серед них є:

– алгоритм неоднозначного шифрування за відкритим ключем на базі розширеної криптографічної схеми Рабіна [11];

– алгоритм неоднозначного шифрування на базі протоколу BCP [12];

– алгоритм неоднозначного шифрування на базі протоколу RD-PKE [13];

– алгоритм неоднозначного шифрування Канетті [14].

З метою визначення можливості застосування методів неоднозначного шифрування для застосування в ІСПДн було проведено оцінку їх характеристик і їх стійкості до вразливостей, наведених вище. Результати аналізу подано в табл. 2.

Таблиця 2 – Результати аналізу засобів неоднозначного шифрування

Параметри аналізу	Алгоритми неоднозначного шифрування			
	Використання фіктивних даних	Використання контейнерів	Комбінація схем шифрування	Побітове шифрування
Сімейство алгоритму	Асиметричні алгоритми	Асиметричні алгоритми	Асиметричні алгоритми	Симетричні, асиметричні Алгоритми
Схема перетворень	$a^x \pmod n$	Інкапсуляція даних у контейнер	$a^x \pmod n$ *Діффі-Хеллмана*	$x \in \{0,1\}^n \to \pi(x) = \begin{cases} 0, \text{умова } 1 \\ 1, \text{умова } 2 \end{cases}$
Наявність ключів шифрування	Так	Так	Так	Так
Стійкість ключів до компрометації	Так	Так	Так	Так
Стійкість до підробки ключів	Так	Розподіл ключа на частини	Хешування секретних параметрів	Так
Стійкість до підбору ключів	Так	Так	Так	Так
Обчислювальна стійкість	Так	Так	Так	Так
Стійкість до застосування примусу	Так	Так	Так	Так
Стійкість до атак на основі відкритих ПДн	Так	Так	Так	Так
Стійкість до атак на основі шифрованих ПДн	Так	Так	Так	Так
Стійкість до атак на основі реверс інжинірингу алгоритму	Так/Ні (залежить від реалізації)	Так/Ні (залежить від реалізації)	Так/Ні (залежить від реалізації)	Так/Ні (залежить від реалізації)
Стійкість до атак MITM	Так	Так	Так	Так

Згідно з наведеними вище даними випливає, що майже усі алгоритми неоднозначного шифрування ґрунтуються на використанні асиметричних схем перетворення даних, тобто їх використання передбачає наявність 2-х та більше ключів шифрування даних, а отже їх можливо використовувати для вирішення питань мережевої безпеки (переважно). Але їх гнучкість дозволяє реалізовувати неоднозначне шифрування даних на базі симетричних алгоритмів. Загалом майже усі проаналізовані вище схеми перетворень можна описати схемою (рис. 6).

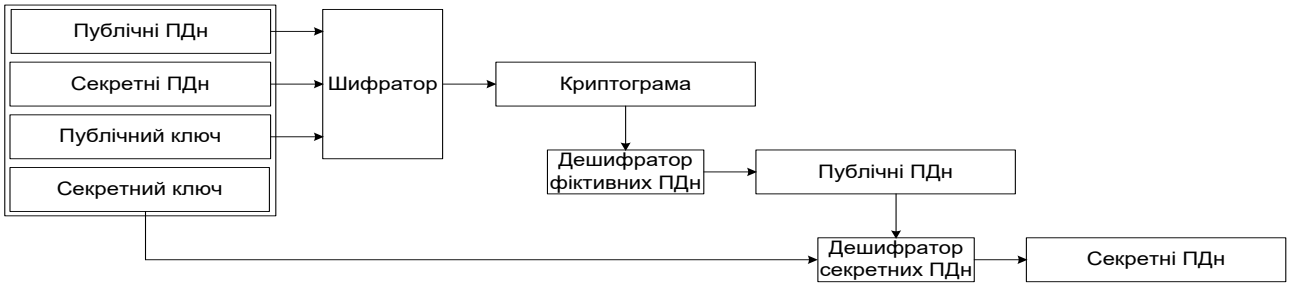

Рис. 6. Загальна схема реалізації неоднозначного шифрування даних з використанням відритого ключа

Наведена вище схема реалізації механізму заперечування наявності даних в ІСПДн дозволяє вирішити проблеми, пов'язані з впливом людського фактору на роботу підсистем захисту ІСПДн, оскільки вони виконують генерацію $4 \cdot N$ повідомлень на етапі дешифрування криптограми і для перевірки усіх варіацій даних, у реальних умовах, зловмисникові знадобиться велика кількість часу та спеціалізоване програмне забезпечення для розпізнавання інформативних складових ПДн. Тобто час, необхідний для їх аналізу, $t \to \infty$.

Приклад 3: застосуємо алгоритм неоднозначного шифрування [12] для захисту інформації в ІСПДн. За секретні дані обрано дані з таблиці T, а для фіктивних – з таблиці M.

Згідно з алгоритмом були генеровані публічний ключ $N = 247$ і секретний ключ $(p,q) = (13,19)$, а також виконано шифрування даних з таблиці T. У результаті чого отримано криптограму C:

$$T = \begin{pmatrix} 171 & 64 & 34 \\ 86 & 240 & 190 \\ 149 & 44 & 23 \end{pmatrix} \quad M = \begin{pmatrix} 236 & 60 & 152 \\ 44 & 240 & 35 \\ 211 & 16 & 41 \end{pmatrix} \quad C = \begin{pmatrix} (201;190) & (228;240) & (184;218) \\ (175;71) & (105;27) & (41;114) \\ (225;44) & (151;17) & (29;37) \end{pmatrix}.$$

Використовуючи особливості цього алгоритму шифрування, виконаємо дешифрування фіктивних ПДн M' з криптограми C, які призначені для отримання зловмисником, у разі застосування ним примушування до оператора ІСПДн:

$$M' = \begin{pmatrix} (236;106;141;11) & (174;187;60;73) & (152;152;95;95) \\ (70;44;203;177) & (240;45;202;7) & (22;35;212;225) \\ (211;55;192;36) & (231;244;3;16) & (41;54;193;206) \end{pmatrix} => \begin{pmatrix} 236 & 60 & 152 \\ 44 & 240 & 35 \\ 211 & 16 & 41 \end{pmatrix}.$$

З отриманих наборів даних оператор обирає істинні M' значення та передає їх зловмисникові як секретні ПДн.

Для відновлення секретних даних з криптограми C оператору необхідно виконати додаткову ітерацію алгоритму, яка здійснює дешифрування секретних ПДн T' з фіктивних M'. У результаті чого були отримані секретні ПДн T':

$$T' = \begin{pmatrix} (171;171;76;76) & (12;64;183;235) & (34;99;148;213) \\ (86;47;200;161) & (240;45;202;7) & (190;190;57;57) \\ (136;149;98;111) & (70;44;203;177) & (205;23;224;42) \end{pmatrix} => \begin{pmatrix} 171 & 64 & 34 \\ 86 & 240 & 190 \\ 149 & 44 & 23 \end{pmatrix}.$$

Якщо у використаному алгоритмі шифрування реалізувати стійкість до атак на основі реверс інжинірингу [17], то отримані зловмисником дані він вважатиме секретними і припинить протиправні дії проти оператора ІСПДн. У протилежному випадку він може продовжити дешифрування даних і з деякою ймовірністю отримає секретні ПДн.

Порівнявши дані з табл. 1-3, які наведено вище, було оцінено рівень надійності вказаних підсистем захисту, у разі їх реалізації в ІСПДн (графічно аналіз надійності підсистем шифрування наведено на рис. 7).

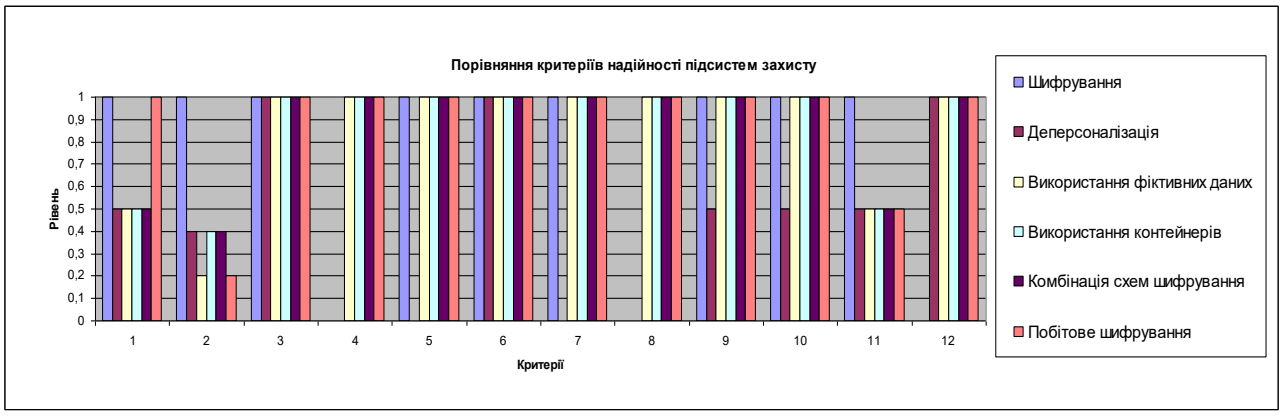

Рис. 7. Порівняння критеріїв надійності підсистем захисту ІСПДн

Порівнявши результати обчислень у прикладах 1-3 і дані гістограми на рис. 7, можна зробити відповідні висновки:

1) алгоритми неоднозначного шифрування реалізовані на базі існуючих криптографічних схем перетворення даних, тобто вони володіють їх перевагами та недоліками (стійкість до атак у них така сама);

2) до ключів обох типів криптографічних систем висуваються однакові вимоги щодо їх генерації, довжини та зберігання, але, на відміну від традиційних криптографічних систем, компрометація ключів в алгоритмах неоднозначного шифрування не є серйозною загрозою для безпеки ІСПДн, адже в них використовується шифрування двох наборів даних (один для зловмисників, інший для оператора ІСПДн);

3) в алгоритмах неоднозначного шифрування присутній надлишок інформації (порівняно з кількістю вхідних даних, кількість вихідних зростає, пропорційно, в N-разів), що може створити значне навантаження на існуючі системи обробки даних;

4) в алгоритмах неоднозначного шифрування реалізовано механізм приховування даних, подібно до методів стенографії (тобто наявність прихованих даних досить складно виявити і ще складніше отримати без відповідного ключа та знання особливостей використаного алгоритму шифрування);

5) в алгоритмах неоднозначного шифрування реалізована досить незначна кількість схем перетворення даних, що пов’язано з ненабуттям ними поширення, і досить складно реалізувати захист даних з використанням властивостей блочних алгоритмів шифрування (але для зберігання ПДн це не критично).

ВИСНОВКИ З ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ

Отже, використання алгоритмів неоднозначного шифрування має свої переваги та особливості реалізації перед традиційними і сучасними підходами до захисту інформації в ІСПДн. Їх основною перевагою є те, що використання дозволяє виключити можливість впливу людського фактору на роботу підсистем захисту в ІСПДн (на відміну від традиційних засобів). Крім того, вони володіють стійкістю криптографічних схем, на базі яких побудовано усі сучасні механізми захисту інформації, а тому забезпечують, щонайменше, той самий

рівень надійності, що й останні. Але невеликий обсяг досліджень у цьому напрямі не дозволяє повною мірою оцінити їх переваги і недоліки при вирішення практичних завдань з інформаційної безпеки.

Окрім того, вони мають досить мале коло застосування через малу кількість механізмів, реалізованих у них (їх обмежений функціонал не дозволяє використовувати їх для захисту «bigdata»). Саме тому вони не набули значного поширення для практичного застосування (порівняно з ними, криптографічний алгоритм RSA більш простий для реалізації та застосування).

Для подальших досліджень у цьому напрямі рекомендована робота з таких питань:

– застосування засобів неоднозначного шифрування в системах (наприклад, засоби радіоелектронної боротьби тощо);

– створення електронних цифрових підписів на базі алгоритмів неоднозначного шифрування;

– адаптація алгоритмів неоднозначного шифрування для захисту «bigdata»;

– розробка та реалізація механізмів автоматичного дешифрування секретних і фіктивних даних;

– підвищення продуктивності алгоритмів шляхом їх оптимізації і використання технологій прискорення обробки даних (паралельні обчислення, апаратне прискорення, тощо);

– дослідження можливості застосування неоднозначного шифрування для захисту від квантових алгоритмів зламу;

– розробка програмного комплексу, який реалізує неоднозначне шифрування даних для захисту інформації з поєднанням технічних, програмних і організаційних заходів захисту.

З огляду на те, що надійність засобів неоднозначного шифрування значно більша за надійність традиційних та сучасних криптографічних систем захисту, їх практичне застосування мало досліджене і вони не набули поширення, то подальші дослідження в даному напрямі є актуальними.

ЛІТЕРАТУРА

1. Верховна рада України. ЗАКОН УКРАЇНИ «Про захист персональних даних». Законодавство України. URL: http://zakon2.rada.gov.ua/laws/show/2297-17 (Дата звернення: 01.01.2017).

2. Кисиль В. Исполнение требований Закона «О защите персональных данных». ЮРИСТ&ЗАКОН. URL: http://vkp.ua/ru/publications/articles/enforcing_the_requirements_of_the_personal_information_protection_act/ (Дата звернення: 01.01.2017).

3. Трубачева С. И. Основные аспекты защиты персональных данных на предприятии. *Вестник Волжского университета им. В. Н. Татищева*. URL: http:// cyberleninka.ru/article/n/osnovnye-aspekty-zaschity-personalnyh-dannyh-na-predpriyatii (Дата звернення: 15.10.2017).

4. Арина Ли. Объем утечек конфиденциальной информации в мире в 2017 году вырос в 8 раз. РБК. URL: http:// www.rbc.ru/technology_and_media/10/10/2017/59db57549a7947f8d8839 ac3 (Дата звернення: 15.10.2017).

5. Мавринская Т. В., Лошкарёв А. В., Чуракова Е. Н. Обезличивание персональных данных и технологии «Больших данных» (bigdata). URL: http:// Scientific Cooperation Center «Interactive plus» (Дата звернення: 15.10.2017).

6. Шамсутдинов Б. Обезличивание персональных данных и data masking. Криптоанархист. URL: http:// crypto-anarchist.blogspot.com/2013/12/data-masking.html (Дата звернення: 15.10.2017).

7. Куракин А. С. Алгоритм деперсонализации персональных данных. *Научно-технический вестник информационных технологий, механики и оптики*. URL: http://

cyberleninka.ru/article/n/algoritm-depersonalizatsii-personalnyh-dannyh (Дата звернення: 15.10.2017).

8. Трифонова Ю. В., Жаринов Р. Ф. Возможности обезличивания персональных данных в системах, использующих реляционные базы данных. *Доклады Томского государственного университета систем управления и радиоэлектроники*. URL: http:// cyberleninka.ru/article/n/vozmozhnosti-obezlichivaniya-personalnyh-dannyh-v-sistemah-ispolzuyus chih-relyatsionnye-bazy-dannyh (Дата звернення: 15.10.2017).
9. Бондаренко К. О. Универсальный быстродействующий алгоритм процедур обезличивания данных. *Известия Южного федерального университета. Технические науки*. URL: http://cyberleninka.ru/article/n/universalnyy-bystrodeystvuyuschiy-algoritm-protsedur-obezli chivaniya-dannyh (Дата звернення: 15.10.2017).
10. Мелихова О. А., Чумичев В. С., Джамбинов С. В., Гайдуков А. Б. Некоторые аспекты криптографического взлома и повышения надежности алгоритмов шифрования. *Молодой ученый.* 2015. №11. С. 392-394.
11. Молдовян Н. А., Горячев А. А., Вайчикаускас М. А. Расширение криптосхемы Рабина: алгоритм отрицаемого шифрования по открытому ключу. *ФГУП «ВИМИ»*. 2014. №2. С. 12–16.
12. Wang J. A, Meng Bo. Encryption Scheme. *Proceedings of the 2009 International Symposium on Information Processing (ISIP'09)*: (Huangshan: P. R. China, 21–23 August 2009). Huangshan, 2009.
13. Ibrahim H. Receiver-deniable Public-Key Encryption. *International Journal of Internet Security*. 2009. Vol. 8, № 2. P. 159–165.
14. Canetti R., Dwork C., Naor M., Ostronsky R. Deniable Encryption. *Advances in Cryptology*. 1997. P. 90–104.
15. Козіна Г. Л., Гальченко А. В. Заперечуване шифрування. *Тиждень науки*: (Запоріжжя, 13–17 квітня 2015 р.). Запоріжжя, 2015.
16. Гальченко А. В., Козіна Г. Л. Модифікація алгоритму заперечуваного шифрування Менга. *Радіоелектроніка, інформатика, управління*. URL: http://cyberleninka.ru/article/n/modi fikatsiya-algoritmu-zaperechuvanogo-shifruvannya-menga (Дата звернення: 15.10.2017).
17. Атака на чёрный ящик. Реверс-инжиниринг виртуализированного и мутированного кода. Habrahabr. URL: http://habrahabr.ru/post/225963/ (Дата звернення: 15.10.2017).

REFERENCES

1. (2017). ZAKON UKRAJINY «Pro zahyst personalnyh danyh». Verxovna rada Ukrajiny. Retrieved from http://zakon2.rada.gov.ua/laws/show/2297-17.
2. Kisyl, V. (2011). Ispolnenie trebovanij Zakona «O zashchite personalnyh danyh». YURYST&ZAKON. Retrieved from http://vkp.ua/ru/publications/articles/enforcing_the_requireme n ts_of_the_personal_information_protection_act.
3. Trubacheva, S. Y. (2010). Osnovnye aspekty zashchity personalnyh dannyh na predpryjatii. Vestnik Volzhskogo universiteta im. V.N. Tatyshcheva. Retrieved from http://cyberleninka.ru/articl e/n/osnovnye-aspekty-zaschity-personalnyh-dannyh-na-predpriyatii.
4. Aryna, Ly (2017). Obiem utechek konfydencyalnoy informacii v mire v 2017 godu vyros v 8 raz. RBK. Retrieved from http://www.rbc.ru/technology_and_media/10/10/2017/59db57549a7947 f8d8839ac3.
5. Mavrynskaya, T. V., Loshkarev, A. V. & Churakova, E. N. (2017). Obezlichivanie personalnyh dannyx i texnologii «Bolshix dannyx» (bigdata). Scientific Cooperation Center «Interactive plus». Retrieved from https://cyberleninka.ru/article/v/obezlichivanie-personalnyh-dannyh-i-tehnologii-bol shih-dannyh-bigdata.
6. Shamsutdynov, B. (2013). Obezlichivanie personalnyh dannyh i data masking. Kryptoanarxyst. Retrieved from http://crypto-anarchist.blogspot.com/2013/12/data-masking.html.
7. Kurakyn, A. S. (2012). Algoritm depersonalizacii personalnyh dannyh. Nauchno-texnycheskiy vestnik informacionnyh texnologiy, mexaniki i optiki. Retrieved from http://cyberleninka.ru/article/n/algoritm-depersonalizatsii-personalnyh-dannyh.
8. Tryfonova, Yu. V. & Zharynov, R. F. (2014). Vozmozhnosti obezlichivaniya personalnyh dannyh v systemah, ispolzuyushchih relyacionnye bazy dannyh. Doklady Tomskogo gosudarstvennogo unyversyteta system upravlenyya y radyoэlektronyky. Retrieved from

http://cyberleninka.ru/article/n/vozmozhnosti-obezlichivaniya-personalnyh-dannyh-v-sistemah-ispolzuyus chih-relyatsionnye-bazy-dannyh.

9. Bondarenko, K. O. (2015). Unyversalniy bystrodejstvuyushhij algorytm procedur obezlichivanija dannyh. Izvestija Juzhnogo federalnogo universiteta. Texnicheskie nauki. Retrieved from http://cyberleninka.ru/article/n/universalnyy-bystrodeystvuyuschiy-algoritm-protsedur-obezlichivaniya-dannyh.
10. Melihova, O. A., Chumichev, V. S., Dzhambinov, S. V. & Gajdukov, A. B. (2015). Nekotorye aspekty kryptograficheskogo vzloma i povishenija nadezhnosti algoritmov shifrovanija. Molodoj uchenyj, No. 11, pp. 392-394 (in Russian).
11. Moldovjan, N. A., Gorjachev, A. A. & Vajchikauskas, M. A. (2014). Rasshyrenye kryptoshemy Rabina: algoritm otriczaemogo shifrovanija po otkrytomu kljuchu. VZI. Zhurnal po voprosam zashchyty informacii. FGUP «VYMY», No. 2, pp. 12–16 (in Russian).
12. Wang, J. A & Meng, Bo. (2009, August). Receiver Deniable Encryption Scheme. Proceedings of the 2009 International Symposium on Information Processing (ISIP'09), (pp. 254–257), Huangshan: P. R. China.
13. Ibrahim, H. (2009). Receiver-deniable Public-Key Encryption. International Journal of Internet Security, Vol. 8, No. 2, pp. 159–165.
14. Canetti, R., Dwork, C., Naor, M. & Ostronsky, R. (1997). Deniable Encryption. Proceedings of Advances in Cryptology, pp. 90–104.
15. Kozina, G. L. & Galchenko, A. V. (2015, April). Zaperechuvane shifruvannja. Tyzhden nauky – 2015: Tezy dopovidej shhorichnoyi nauk.-prakt. konf. vykladachiv, naukovciv, molodyh uchenyh, aspirantiv, studentiv ZNTU, Zaporizhzhya.
16. Galchenko, A. V. & Kozina, G. L. (2016). Modifikacija algorytmu zaperechuvanogo shyfruvannya Menga. Radioelektronika, informatyka, upravlinnya. Retrieved from http://cyberleninka.ru/article/n/modifikatsiya-algoritmu-zaperechuvanogo-shifruvannya-menga.
17. (2014). Ataka na chernij yashhik. Revers-inzhiniring virtualizirovannogo i mutirovannogo koda. Habrahabr. Retrieved from http://habrahabr.ru/post/225963/.

УДК 539.3

ОПРЕДЕЛЕНИЕ ОБЛАСТЕЙ УСТОЙЧИВОСТИ КОНИЧЕСКОЙ ОБОЛОЧКИ ПРИ КОМБИНИРОВАННОМ НАГРУЖЕНИИ НА БАЗЕ ГИБРИДНОГО АСИМПТОТИЧЕСКОГО ПОДХОДА

Грищак В. З., д. т. н., профессор, Дьяченко Н. Н., к. ф.-м. н., доцент

Запорожский национальный университет,
ул. Жуковского, 66, г. Запорожье, 69600, Украина

dyachenkonata69@gmail.com

Рассматривается линейная задача устойчивости конической оболочки при комбинированном нагружении тремя усилиями: всесторонним внешним давлением, осевым сжатием и крутящим моментом. Выведено обыкновенное дифференциальное уравнение четвертого порядка, к которому сводится система уравнений в частных производных полубезмоментной теории устойчивости оболочки. Задача решается с помощью ВКБ метода, гибридного ВКБ-Галеркин метода и метода конечных разностей. Проведен сравнительный анализ результатов, полученных разными методами. Выявлено преимущество асимптотического гибридного метода перед другими методами. Построены линии уровня поверхности устойчивости. Выявлено влияние угла конусности и длины образующей конической оболочки на ее устойчивость.

Ключевые слова: коническая оболочка, устойчивость оболочки, комбинированное нагружение, поверхность устойчивости, гибридный асимптотический ВКБ-Галеркин метод.