ВИЗНАЧЕННЯ ДОСТОВІРНОСТІ ДРУКОВАНИХ ДОКУМЕНТІВ МЕТОДОМ ПОПІКСЕЛЬНОГО ПОРІВНЯННЯ

Іванна Дронюк[1], Марія Назаркевич[1], Юрій Опотяк[2]

[1]Національний університет «Львівська політехніка», Україна
[2]Науково-дослідний центр телекомунікаційних систем та мереж зв'язку Одеської національної академії зв'язку ім. О.С. Попова, Україна

ДРОНЮК Іванна Мирославівна, к.ф.-м.н., доцент

Рік та місце народження: 1961 рік, м. Львів, Україна.
Освіта: Львівський державний університет ім.І.Франка (з 2000 року – Львівський державний університет ім.І.Франка Національний авіаційний університет), 1982 рік.
Посада: доцент кафедри автоматизовані системи управління Національного університету «Львівська політехніка» з 2000 року.
Наукові інтереси: математичне моделювання складних систем, захист інформації.
Публікації: більше 70 наукових публікацій, серед яких навчальні посібники, наукові статті та патенти.
E-mail: idronjuk@polynet.lviv.ua

НАЗАРКЕВИЧ Марія Андріївна, к.т.н., доцент

Рік та місце народження: 1973 рік, м. Львів, Україна.
Освіта: Українська академія друкарства, 1995 рік.
Посада: доцент кафедри інформаційних технологій видавничої справи Національного університету «Львівська політехніка» з 2005 року.
Наукові інтереси: захист друкованих документів, додрукарська підготовка макетів документів, методи графічного захисту.
Публікації: більше 100 наукових публікацій, серед яких навчальний посібник, монографія.
E-mail: nazarkevich@mail.ru

ОПОТЯК Юрій Володимирович, к.т.н., с.н.с.

Рік та місце народження: 1964 рік, м. Львів, Україна.
Освіта: Львівський політехнічний інститут, 1986 рік.
Посада: старший науковий співробітник науково-дослідного центру телекомунікаційних систем та мереж зв'язку Одеської національної академії зв'язку ім. О.С.Попова з 2010 року.
Наукові інтереси: інформаційна безпека, розробка засобів збору та обробки інформації.
Публікації: більше 40 наукових публікацій, серед яких наукові статті, тези доповідей та патенти на винаходи.
E-mail: yuvoua@yahoo.com

Анотація. *В роботі представлений метод визначення достовірності друкованого документа, який ґрунтується на критерії коефіцієнта відношення сигналу до шуму, що обчислюється з попіксельного порівняння контрольованого та еталонного зображень документів. Розроблено алгоритм суміщення оцифрованих документів і попіксельної перевірки тотожності відповідних зображень документів та опрацьовано програмний засіб, який реалізує ці алгоритми з метою визначення достовірності контрольованого документу. Ефективність розробленого програмного продукту була доведена на основі експериментів, які описані в даній роботі*

Ключові слова: *ідентифікація друкованих документів, коефіцієнт PSNR, інформація на матеріальних носіях, графічний захист.*

Вступ

На сьогодні застосовуються такі технічні рішення для реалізації порівняльного дослідження документів на предмет фальсифікації [1]. Методика дослідження складається з чотирьох етапів: 1) оцифровування документів наданих на дослідження об'єктів; 2) приведення документів до однакової взаємної орієнтації на площині та їх

кольорова корекція; 3) накладання зображень об'єктів, що ідентифікуються; 4) оцінювання результатів накладання – фахівець повинен оцінити збіг (або розбіжність) контурів деталей об'єктів та їх кольорових характеристик. У багатьох галузях виникає проблема визначення достовірності документа в цілому. Для її розв'язання опрацьовано метод та відповідне програмне забезпечення, тобто засіб, що на основі попіксельного порівняння оригінального та контрольованого зображення документів встановлює його достовірність. Запропонований метод, подібний до описаного вище методу з криміналістики, але реалізований з допомогою сучасних інформаційних технологій.

Основна частина дослідження

Розглянемо документ П. Будемо вважати його оцифроване представлення еталонним зображенням і позначатимемо Р. Нехай еталонне зображення має розмір $m_p \otimes n_p$ пікселів. Оцифроване еталонне зображення документу розглядаємо у градаціях сірого (для випадку 8 біт/піксель маємо 256 градацій). Це означає, що для кожної поточної точки оцифрованого документу з координатами (x, y) задана функція $P(x, y)$,

$\{P(x,y):\{1,\ldots,m_p\}\otimes\{1,\ldots,n_p\}\to\{0,\ldots,255\}\}$

зі значенням градацій сірого. Введемо у розгляд контрольований документ $П_0$. Для визначення його достовірності необхідно також отримати оцифроване зображення, яке будемо позначати P_0. Будемо вважати, що оцифроване контрольоване зображення Р0. документу П0 має той самий розмір $m_p \otimes n_p$ пікселів, що і еталон Р. Умовне зображення документів показано на рис.1а). Для кожної поточної точки оцифрованого контрольованого документа з координатами (x, y) задана функція $P_0(x, y)$,

$\{P_0(x,y):\{1,\ldots,m_p\}\otimes\{1,\ldots,n_p\}\to\{0,\ldots,255\}\}$

аналогічна функції $P(x, y)$. На основі введених функцій $P(x, y)$ та $P_0(x, y)$ було запропоновано обчислення коефіцієнта PSNR, значення якого є критерієм визначення достовірності друкованого документу у запропонованому методі.

Для реалізації методу попіксельного порівняння означимо коефіцієнт PSNR, відношення сигналу до шуму [5] за формулою:

$$PSNR = 10\log_{10}\frac{MaxP^2 m_p n_p}{\sum\limits_{x=1,y=1}^{m_p n_p}\left(P(x,y)-P_0(x,y)\right)^2}, \qquad (1)$$

де $MaxP = \{\max\limits_{x,y} P_0(x,y) \,|\, x=1,\ldots,m_p,\ y=1,\ldots,n_p\}$ — максимальне значення градації сірого у контрольованому зображенні. Отже критерієм визначення достовірності друкованого документа вибрано значення коефіцієнта PSNR: чим більше значення коефіцієнта PSNR, тим ближче контрольоване зображення до еталонного При проведенні досліджень важливо екпериментальним чином визначити порогове значення $PSNR_{пор}$. Якщо PSNR >$PSNR_{пор}$, вважаємо документ достовірним, у протилежному випадку PSNR <=$PSNR_{пор}$ документ не є достовірним.

Для реалізації алгоритму визначення достовірності друкованого документу надзвичайно важливою є реалізація якнайточнішого суміщення зображень Р та P_0. Для процедури суміщення запропоновано наступний алгоритм. Вибирається точка M_0 на контрольованому зображенні P_0. та задається розмір контрольного вікна r_k (наприклад, 20 пікселів) та точка М на еталонному зображенні. Задається також розмір вікна пошуку для контролю суміщення d_k, причому $d_k > r_k$.

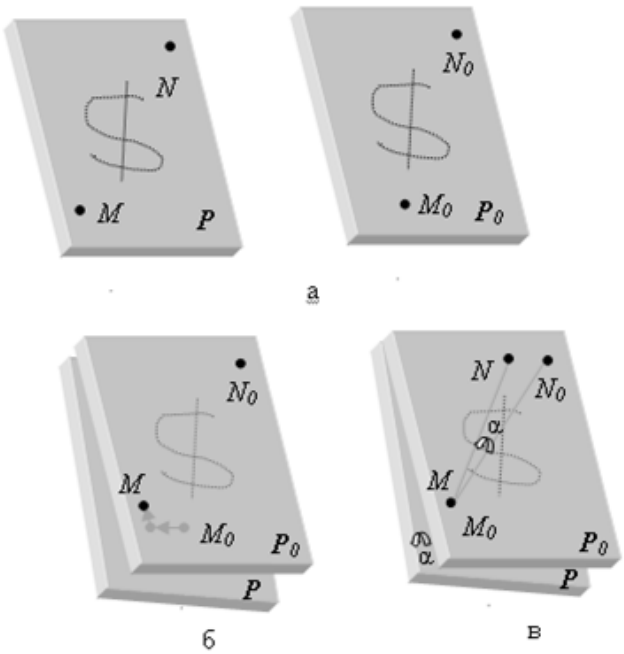

Рис. 1 Реалізація алгоритму суміщення еталонного **Р** та контрольованого **P_0** зображень документів а) документи без суміщення; б) суміщенння зсуву; в) суміщення за поворотом

У вікні розміром $d_k \times d_k$, що містить контрольну точку M_0, знаходимо на еталонному зображенні вікно, яке максимально збігається з контрольним вікном за критерієм максимальної кореляції, відповідно до формули

$$\rho(d_k) = \max_{r_k}\rho(r_k, d_k) = \frac{\sum\limits_{x=1,y=1}^{r_k}(P(x,y)-\bar{P}_0)(P_0(x,y)-\bar{P})}{\sqrt{\sum\limits_{y=1}^{r_k}\sum\limits_{x=1}^{r_k}(P(x,y)-P_0(x,y))^2}}, \qquad (2)$$

$r_k = 1,\ldots,d_k$.

У формулі (2) $\bar{P}, \bar{P}_0$ - середнє значення функцій $P(x, y)$ та $P_0(x, y)$ на квадраті зі стороною r_k. Після визначення коефіцієнта максимальної кореляції (2) проводимо суміщення зображень (зсув по горизонталі та вертикалі рис.1б) таким чином, щоб вибрані контрольні точки та вікна повністю збігалися. Вибір більшого розміру вікна пошуку (в пікселах) для процедури суміщення еталонного і контрольованого зображень дозволяє точніше

визначити взаємне зміщення зображень при його великому значенні, але збільшує час роботи алгоритму.

Для суміщення зображень за поворотом задається друга контрольна точка N0 на зображенні P0 та N на зображенні P у протилежному від точки M0 куті зображення та розмір вікна пошуку для контролю суміщення за поворотом d_p, причому $d_p > d_k$. Аналогічно, як для першої контрольної точки M0, у вікні розміром $d_p \times d_p$ знаходимо квадрат, що максимально збігається з контрольним вікном за критерієм кореляції (2), де у формулі (2) замість d_k беремо значення d_p. Утворений кут M_0N_0N між першою та другою контрольними точками на еталонному та контрольному зображеннях є шуканим кутом повороту (при цьому точки M_0 та M вже суміщено рис. 1в). Повертаємо контрольне зображення на знайдений кут за відомими формулами повороту площини [2] з центром у першій контрольній точці M_0. На основі описаного алгоритму суміщення еталонного та контрольованого зображень та формули (1) обчислення коефіцієнта PSNR, було розроблено відповідне програмне забезпечення, робоче вікно якого з результатами розрахунку показано на рис. 2. Для прикладу, для обробки документу $П_0$ з відповідним зображенням P_0 розміром 900x800 пікселів на ПК з процесором Intel Celeron SU2300 необхідно для обчислення суміщення зсуву 27 с, для обчислення суміщення за поворотом 74 с, час обчислення коефіцієнта PSNR 74 с.

Для доведення ефективності розробленого методу та відповідного програмного продукту було проведено наступні експерименти.

Експеримент проводився на 15 друкованих документах, які були захищені за технологією запропонованою у [3]. Експеримент включає наступні кроки:

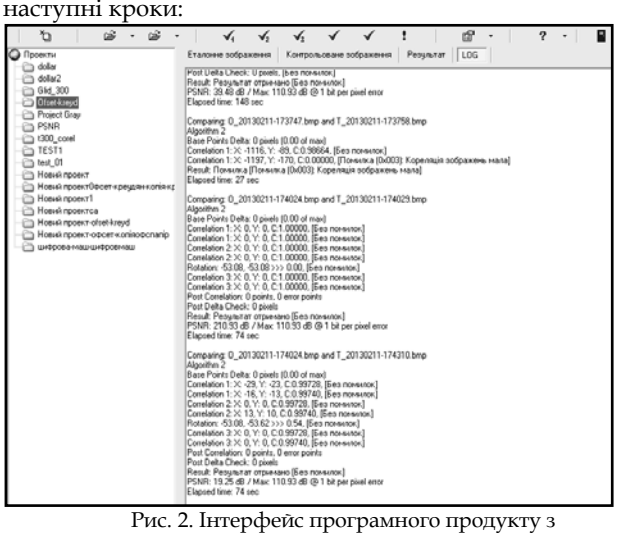

Рис. 2. Інтерфейс програмного продукту з результатами ідентифікації

1. Сформовано файл з захистом у векторному форматі;

2. Виведено друкарські плівки з макетом захищеного документу;

3. На основі виведених плівок видрукувано оригінали документів офсетним способом друку на двох різних типах паперу.

4. Реалізовано 4 описаних нижче атак на кожний з видрукуваних документів:

− підробка документа на кольоровому ксероксі;

− підробка документа на одноколірному ксероксі;

− підробка документа на різографі;

− часткова підчистка документа;

5. Підроблений документ перевірявся на достовірність за допомогою розробленого програмного продукту з обчисленням коефіцієнта PSNR.

6. Висновок про достовірність.

Способи підробки документів залежать від рівня технічного розвитку суспільства. Репрографією прийнято називати відтворення інформації шляхом її репродукування методами електрографії. За даними приведеними у роботі [4] приблизно 30 відсотків усіх фальшивих банкнот в світі виготовляється за допомогою кольорової комп'ютерної та копіювальної оргтехніки, тобто засобами репрографії. За останні роки у Росії цей показник досяг 98 відсотків при підробці національних грошей, в Україні - 70 відсотків. Ці дані підтверджуються дослідженнями [1], де вказано, що переважна кількість підробок отримується на принтерах.

Тому у даній роботі проводились експерименти щодо дослідження ефективності запропонованого методу для визначення підробок документів, зроблених способом репрографії. У табл. 1 та 2 представлено результати проведених експериментів ідентифікації документів з графічними методами захисту. Оригінали документів виведено машиною цифрового друку Xerox Color 550/560, різографом Duplicator DD-S 850, принтером Hewlett Packard- 5200 на двох типах паперу – крейдованому (папір № 1) та офсетному (папір № 2). Здійснено повну підробку документа репрографічним методом на двох видах ксерокопіювальної техніки, найбільш розповсюдженої сьогодні: кольоровому ксероксі Konica Minolta та чорно-білому ксероксі фірми Canon IR2022. Було проведено експерименти визначення достовірності документів методом повного попіксельного порівняння еталонного та контрольованого зображень на основі використання опрацьованого програмного продукту.

У результаті експериментів визначався коефіцієнт відношення максимально можливого значення сигналу до шуму *PSNR*, який взято за показник ідентифікації. Будемо вважати, що більше значення коефіцієнта *PSNR*, відповідає кращому результату визначення достовірності. Вважаємо пороговим значенням для коефіцієнта $PSNR_{пор}$ =20, якщо оригінал документу надрукований офсетним способом друку. У випадку значення коефіцієнта *PSNR* в межах [20; 255] будемо вважати документ достовірним. Якщо $PSNR \in [6;20]$, то вважаємо документ не достовірним, тобто підробленим. Якщо

значення коефіцієнта PSNR $\in[0;6]$, то вважаємо що контрольований документ не є достовірним, і підробка виконана дуже низькоякісним способом.

За даними експериментів випливає, що при виготовленні копії документа ксерокопіюванням значення коефіцієнта *PSNR* було в межах 18-0. Результати експериментів приведені у таблицях 1,2. Порівняння результатів показує, що офсетний папір є дещо стійкішим до атак, ніж крейдований папір. Для візуалізації результати проведених експериментів показані на рис.3-6. Проведені дослідження показують, що розроблений програмний продукт успішно визначає підроблені документи (значення коефіцієнта PSNR менше $PSNR_{пор}$ =20 для всіх видів підробок)

Таблиця 1

Експериментальні дослідження результатів визначення достовірності документа, виготовленого репрографією на крейдованому папері

Види атак	Засоби оперативної поліграфії					
	Різограф Duplicator DD-S 850		Принтер HP-5200		Машина цифрового друку Xerox Color 550/560	
Оригінал (атака відсутня)	PSNR, дБ	Відносний коефіцієнт,%	PSNR. дБ	Відносний коефіцієнт,%	PSNR, дБ	Відносний коефіцієнт, %
	210,52	100	210,5	100	210,89	100
Підробка документа на кольоровому ксероксі; Konica Minolta	9,66	4,5	7,25	3,4	9,47	4,4
Підробка документа на одноколірному ксероксі; Canon IR2022	10,29	4,8	0	0	7,55	3,5

Таблиця 2

Експериментальні дослідження результатів визначення достовірності документа, виготовленого репрографією на офсетному папері

Види атак	Засоби оперативної поліграфії					
	Різограф Duplicator DD-S 850		Принтер HP-5200		Машина цифрового друку Xerox Color 550/560	
Оригінал (атака відсутня)	PSNR, дБ	Відносний коефіцієнт,%	PSNR, дБ	Відносний коефіцієнт,%	PSNR, дБ	Відносний коефіцієнт, %
	210,02	100	210,58	100	210,64	100
Підробка документа на кольоровому ксероксі; Konica Minolta	8,06	3,8	8,98	4,2	0	0
Підробка документа на одноколірному ксероксі; Canon IR2022	6,28	2,9	6,79	3,2	0	0

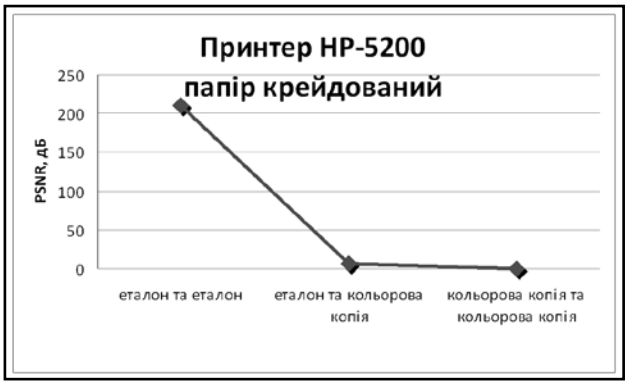

Рис. 3. Експериментальні дослідження результатів визначення достовірності документу для оригіналу виготовленого принтером Hewlett Packard-5200 на крейдованому папері

Рис. 4. Експериментальні дослідження результатів визначення достовірності документу для оригіналу виготовленого на машині цифрового друку Xerox- Color 550/560 на офсетному папері

Рис. 5. Експериментальні дослідження результатів визначення достовірності документу для оригіналу виготовленого машиною цифрового друку Xerox- Color 550/560 на крейдованому папері

Рис.6. Експериментальні дослідження результатів визначення достовірності документу для оригіналу виготовленого різографом Duplicator DD-S 850 на крейдованому папері

У дослідженнях показаних на рис.3 - 6 проведено аналіз атак у вигляді повної підробки документу. Разом з тим актуальним є дослідження часткової підробки.

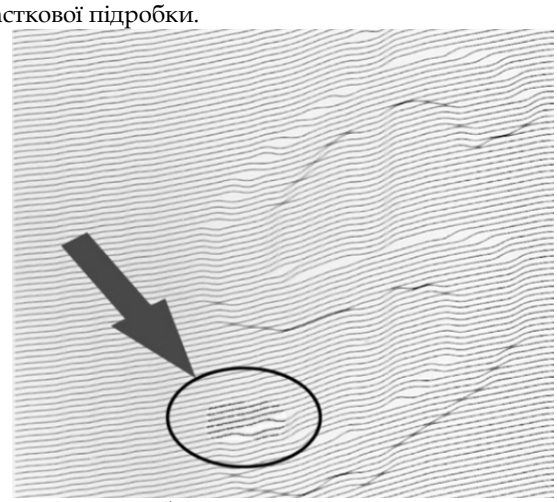

Рис.7. Приклад роботи програмного продукту зі знайденою областю підчистки документу

Як зазначено у праці [1] часткова підробка є досить розповсюдженим видом підробки, найчастіше це намагання змінити первісний номінал справжньої банкноти на більший. Також розповсюджена заміна реквізитів документів та інформації на документах шляхом підчистки. Розроблений програмний продукт також дає можливість виявити таку підробку. Для цього у даному програмному продукті передбачена можливість зміни кольору у області документа, де була здійснена атака. На рис.7 показаний приклад роботи програмного продукту зі знайденою областю підчистки, яку програма позначує червоним кольором.

Висновки

На основі алгоритму суміщення зображень оцифрованого оригіналу документу і його копії та попіксельному порівнянні цих зображень реалізовано метод визначення достовірності друкованого документу. Критерієм порівняння вибрано, обчислений для всіх пікселів оригіналу та копії, коефіцієнт відношення сигналу до шуму PSNR на основі визначення градацій сірого. Грунтуючись на цьому методі опрацьовано відповідне програмне забезпечення. Доведено ефективність роботи програми на основі проведених експериментальних досліджень. Для усіх підробок коефіцієнт PSNR був нижчий визначеного порогового значення. Показано також, що розроблений програмний продукт може бути використаний для визначення часткових підчисток в документах.

Література

[1] Воробей О.В. Техніко-криміналістичне дослідження документів/ О.В. Воробей І.М. Мельников О.Г. Волошин. – Київ: Центр учбової літератури, 2008 . – 304 с.

[2] Корн Г.А. Справочник по математике для научных работников и инженеров / Г. А. Корн, Т. М. Корн. — М. : Наука, 1974. — 832 с..

[3] Дронюк І. Розробка методів захисту документів засобами Ateb-функцій / І. Дронюк, М.Назаркевич // Вісник Східноукраїнського національного університету ім. В.Даля. Информационные технологии и безопасность в управлении. – 2007. – № 5 (111). – С. 44–48.

[4] Петряєв С.Ю. Способи підробки паперових грошових знаків // Вісник Національного технічного університету України «Київський політехнічний інститут». Політологія. Соціологія. Право: Зб. Наук.Праць. – Київ: ІВЦ «Політехніка», 2009. - №4 – С. 2-10.

[5] Salomon David Data Compression: The Complete Reference/Springer, 2007 - 1092 с.

УДК 003.26:004.056.55:621.39 (045)

Дронюк И.М., Назаркевич М.А., Опотяк Ю.В. Определение достоверности печатных документов методом попиксельного сравнения

Аннотация. *В работе предложен метод определения достоверности печатного документа, который основан на критерии коэффициэнта отношения сигнала и шума, вычисляемого на основании попиксельного сравнения контролируемого и эталонного изображений документов.*

Разработан алгоритм совмещения оцифрованных документов и попиксельного сравнения соответствующих изображений документов и разработан программный продукт, который реализирует эти алгоритмы с целью определения достоверности контролируемого документа. Эффективность разработанного программного продукта была доказана с помощью проведенных экспериментов, которые описаны в статье.
Ключевые слова: *идентификация печатных документов, коэффициент PSNR, информация на материальных носителях, графические методы защиты.*

Dronjuk I.M., Nazarkevych M.A., Opotiak Yu.V. Determination of the printed documents reliability by the per-pixel comparing
Abstract. *The paper presents a method of determining authenticity of a printed document, based on the signal-to-noise ratio criteria, which is calculated from pixel by pixel comparison of controlled and reference document images. The algorithm combines digitized documents and pixel by pixel identity checking of the appropriate document images, and processes the software tool that implements these algorithms on purpose to determine authenticity of the controlled document. Effectiveness of the software product was proved on the basis of experiments described in this paper.*
Key words: *authenticity of a printed document, coefficient PSNR, high-security printing.*

Отримано *16 січня 2013 року*, затверджено редколегією *20 лютого 2013 року*

ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТНОЙ НАДЕЖНОСТИ ЕДИНИЧНОЙ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ИЗ РЕАЛЬНЫХ ПОПЫТОК ВЗЛОМА

Борис Журиленко

Национальный авиационный університет, Україна

ЖУРИЛЕНКО Борис Евгеньевич, к.ф.-м.н., доцент, с.н.с.

Год и место рождения: 1946 год, г. Чугуев Харьковской области, Украина.
Образование: Киевский государственный университет им.Т.Г.Шевченко, 1974 год.
Должность: доцент кафедры методов защиты информации с 2003 года.
Научный интерес: методы съема и методы технической защиты информации.
Публикации: более 80 научных статей и патентов на изобретения.
E-mail: zhurilenko@mail. ru

Аннотация. *В результате проведенной работы предложен метод для определения вероятностной надежности технической защиты информации на основании реальных попыток взлома. Предложенный метод позволяет оценить вероятностную надежность единичных систем защиты, а при установке ее на нескольких объектах предсказать не только попытку, но и время, при которых вероятен взлом на других объектах.*

Ключевые слова: *защита информации, надежность, вероятность взлома, комплекс технической защиты информации.*

Введение

Современный этап выбора, исследования, проектирования, создания и эксплуатации комплекса технической защиты информации (КТЗИ) требует использования данных, ориентированных на специально проведенные экспериментальные исследования или на реальные результаты взлома используемых защит. Такой подход позволит сэкономить финансовые ресурсы, провести исследования КТЗИ, выработать рекомендации для его модернизации или новые требования для его разработки. Основными трудностями, связанными с реальными результатами взлома используемых защит, является необходимость взлома защиты и, естественно, невозможность сбора статистических данных о результатах взлома, так как такая защита после взлома не может использоваться в дальнейшем. Проведение специальных экспериментальных исследований – это фактически проведение попыток взлома, которые требуют соответствующего уровня секретности сохранения методов и результатов исследований, что не всегда может быть обеспечено с помощью