Документ складається з тексту, електронного підпису та сертифіката користувача, який містить дані користувача, його ідентифікаційне ім'я та відкритий ключ дешифрування для перевірки підпису адресатом документа [2].

Важливою характеристикою методів шифрування є їх криптографічна стійкість, тобто стійкість до дешифрування без ключа, яка визначається як кількість обчислювальних та інших ресурсів для такого дешифрування.

Порядок здійснення криптографічного захисту інформації з обмеженим доступом використовуються криптосистеми і засоби криптографічного захисту допущені до експлуатації Державної службою спеціального зв'язку та захисту інформації України, які мають сертифікат відповідності.

Таким чином, для шифрування з метою передачі інформації в інформаційних мережах доцільно застосовувати асиметричні методи, а для шифрування з метою зберігання інформації – симетричні. Що ж стосується програм для шифрування інформації, то для захисту інформації, яка використовується органами внутрішніх справ, допустимим є використання лише програмних засобів криптографічного захисту інформації, які сертифіковані в Україні.

Список використаних джерел:

1. Зачек О. І. Криптографічний захист інформації у діяльності органів внутрішніх справ. Науковий вісник Львівського державного університету внутрішніх справ. серія юридична. 2014. Вип. 2. С. 91–99.

2. Клімушин П. С. Стратегії та механізми електронного урядування в інформаційному суспільстві. Монографія. Харків. Вид-во ХарРІ НАДУ «Магістр», 2016. 524с.

УДК 343.98

ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ МОЖАЄВ
доктор технічних наук, професор, професор кафедри інформаційних систем факультету №4, Харківського національного університету внутрішніх справ,
МИХАЙЛО ОЛЕКСАНДРОВИЧ МОЖАЄВ
кандидат технічних наук, завідувач лабораторії комп'ютернотехнічних, телекомунікаційних досліджень та досліджень видео-, звукозапису Харківського науково-дослідного інституту судових експертиз ім. Засл. проф. М.С. Бокаріуса
МИХАЙЛО ОЛЕКСАНДРОВИЧ ЛОГВИНЕНКО завідувач сектору комп'ютернотехнічних, телекомунікаційних досліджень та досліджень видео-, звукозапису Харківського науково-дослідного інституту судових експертиз ім. Засл. проф. М.С. Бокаріуса

АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗНИЩЕННЯ ІНФОРМАЦІЇ З МАГНІТНИХ НОСІЇВ ІНФОРМАЦІЇ

Одним із основних завдань, що вирішуються в межах комп'ютерно-технічної експертизи, є встановлення фактів знищення інформації. Органи

досудового розслідування все частіше ставлять на вирішення питання «Чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації?». Не зважаючи на наявність зазначеного питання у Науково-методичних рекомендаціях з питань підготовки та призначення судових експертиз та експертних досліджень, затвердженої наказом Міністерства юстиції України від 8 жовтня 1998 року № 53/5 (зі змінами та доповненнями) для його вирішення повністю відсутня методична база і питання вирішується виключно на основі спеціальних знань кожного експерта, що стикається з даною проблемою.

Існує ряд методів знищення інформації, що зберігається на жорсткому диску. Ці методи можна умовно розділити за методом впливу на носій:

• програмні методи - засновані на використанні стандартних команд управління НЖМД;

• апаратні методи - реалізуються за допомогою спеціального обладнання, що впливає на магнітні диски НЖМД. За способом впливу апаратні методи класифікуються на кілька підгруп:

• методи, перебудовують доменну структуру магнітного носія без руйнування його конструкції;

• методи, пов'язані з руйнуванням конструкції носія.

Програмні методи знищення інформації

Всі програмні методи знищення інформації можна за ступенем на-надійності розділити на 3 рівні:

Рівень 0. Найбільш проста і часто застосовуєма форма знищення інформації на НЖМД. Замість повного перезапису жорсткого диска в завантажувальний сектор, основну і резервну таблиці розділів записується послідовність нулів. Тим самим ускладняється доступ до даних, що зберігаються на диску. Самі данні не знищуються. Повний доступ до інформації на НЖМД легко відновлюється за допомогою посекторного читання.

Рівень забезпечує найбільшу швидкість, але не може використовуватися при обробці інформації, витік якої небажана.

Рівень 1. Запис послідовності нулів або одиниць в сектора, які містять інформацію, яку потрібно знищити. Програмний доступ до перезаписаних даних неможливий. Однак існує можливість відновлення інформації після перезапису за рахунок залишкової намагніченості крайових областей дискових доріжок, несе інформацію про попередні записи.

Швидкість знищення інформації значно нижче, ніж в попередньому рівні і визначається швидкістю роботи НЖМД (в основному швидкістю запису).

Рівень 2. Використання декількох циклів перезапису інформації. Зі збільшенням числа циклів перезапису ускладняється завдання відновлення видалених даних. Це обумовлюється природним дрейфом друкарській головки НЖМД під час кожного наступного циклу. Імовірність перезапису

крайових областей доріжок зростає. Отже, різко підвищується складність процесу відновлення знищених даних.

Повної гарантії незворотного руйнування інформації немає і в цьому випадку, оскільки програмно неможливо управляти траєкторією руху блоку головок НЖМД і процесом перемагнічування бітових інтервалів. Крім того, знищення інформації ускладнено через складність оцінки факторів, що впливають на точність позиціонування головок.

Недоліком методів цього рівня є низька швидкість знищення інформації.

Апаратні методи знищення інформації

Підвищену надійність знищення інформації, що зберігається на жорсткому диску, забезпечують апаратні методи. Недоліком цих методів є повне або часткове руйнування накопичувача.

Перебудова доменної структури магнітного носія

Оптимальним підходом для забезпечення надійного знищення інформації без фізичного знищення носія є використання методів, що призводять до перебудови структури магнітного матеріалу робочих поверхонь носія. Для цього необхідно усунути неоднорідності вектора намагніченості на доріжках НЖМД. Зміна структури намагніченості магнітного шару може бути виконано кількома принципово різними способами:

• шляхом швидкого нагрівання матеріалу робочого шару носія до точки втрати намагніченість носія (точки Кюрі);

• шляхом розмагнічування робочих поверхонь носія;

• шляхом намагнічування робочих поверхонь носія до максимально можливих значень намагніченості (насичення);

• комбінований. Нагрівання і намагнічування, або нагрівання і розмагнічування.

Руйнування конструкції носія

Методи цієї групи застосовують, коли необхідна гарантія знищення інформації. Вони підрозділяються на:

• механічні;

• хімічні - руйнування робочого шару або основи носія за допомогою хімічно агресивних середовищ;

• термічні - метод полягає в нагріванні носія до температури плавлення в спеціальних печах. Гарантія знищення інформації може бути отримана при розігріві носія до температури 800-1000'С;

• радіаційні - руйнування носія за допомогою використання іонізуючих випромінювань.

Таким чином, були розглянуті існуючи методи знищення інформації з магнітних носіїв інформації.