

05.13.04  
K-143

ՀԱՅՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱՅԻ  
ԻՆՖՈՐՄԱՏԻԿԱՅԻ ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ  
ՊՐՈՔԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

---

ՂԱԶԱՐՅԱՆ Հայկ Լևոնի

ԹԱՔՆԱԳՐԱՅԻՆ ՖԱՅԼԱՅԻՆ ՀԱՄԱԿԱՐԳԵՐԻ ՆԱԽԱԳԾՄԱՆ ՍԿԶԲՈՒՆՔՆԵՐԻ ԵՎ  
ԿԱՅՈՒՆՈՒԹՅԱՆ ԳՆԱՀԱՏՄԱՆ ՄԵԹՈԴՆԵՐԻ ՀԵՏԱԶՈՏՈՒՄ ԵՎ ՄՇԱԿՈՒՄ

Ե.13.04 – «Հաշվողական մեքենաների, համալիրների, համակարգերի  
և ցանցերի մաթեմատիկական և ծրագրային ապահովում»  
մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի  
գիտական աստիճանի հայցման ատենախոսության

ՄԵՂՄԱԳԻՐ

Երևան – 2009

---

ИНСТИТУТ ПРОБЛЕМ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ  
НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК РА

---

КАЗАРЯН Айк Левонович

ИССЛЕДОВАНИЕ И РАЗРАБОТКА ПРИНЦИПОВ ПРОЕКТИРОВАНИЯ И МЕТОДОВ  
ОЦЕНКИ СТОЙКОСТИ СТЕГАНОГРАФИЧЕСКИХ ФАЙЛОВЫХ СИСТЕМ

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических  
наук по специальности 05.13.04 – «Математическое и программное  
обеспечение вычислительных машин, комплексов, систем и сетей»

Ереван – 2009

Ատենախոսության թեման հաստատվել է Հայաստանի պետական ճարտարագիտական համալսարանում (Պոլիտեխնիկ):


Գիտական ղեկավար՝ տ.գ.թ., դոցենտ Գ.Բ. Մարգարով

Պաշտոնական ընդդիմախոսներ՝ տ.գ.դ., ՀՀ ԳԱԱ ակադեմիկոս  
Գ.Հ. Խաչատրյան  
տ.գ.թ. Խ.Գ. Շարոյան

Առաջատար կազմակերպություն՝ «Կապի միջոցների գիտա-  
հետազոտական ինստիտուտ» ՓԲԸ

Պաշտպանությունը կայանալու է՝ 18 դեկտեմբերի 2009թ. ժ. 16<sup>00</sup>-ին ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում գործող 037 «Ինֆորմատիկա և հաշվողական համակարգեր» մասնագիտական խորհրդի նիստում, հետևյալ հասցեով՝ Երևան, 0014, Պ. Սևակ 1:

Ատենախոսությանը կարելի է ծանոթանալ ինստիտուտի գրադարանում:  
Մեղմագիրն առարված է՝ 18 նոյեմբերի 2009թ:

Մասնագիտական խորհրդի գիտական քարտուղար,  
Ֆ.-մ.գ.դ., պրոֆեսոր  Ս.Ե. Հարոյանյան

Тема диссертации утверждена в Государственном Инженерном Университете Армении (Политехник).

Научный руководитель: к.т.н., доцент Г.И. Маргаров


Официальные оппоненты: д.т.н., академик НАН РА  
Г.Г. Хачатрян  
к.т.н. Х.Г. Шароян

Ведущая организация: ЗАО «Научно-исследовательский институт связи»

Защита состоится 18 декабря 2009г. в 16<sup>00</sup> на заседании Специализированного совета 037 «Информатика и вычислительные системы» Института проблем информатики и автоматизации НАН РА по адресу: 0014, г. Ереван, ул. П. Севака 1.

С диссертацией можно ознакомиться в библиотеке института.

Автореферат разослан 18 ноября 2009г.

Ученый секретарь специализированного совета  
д.ф.-м.н., профессор  М. Е. Арутюнян



4792-2009

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В последние годы в связи с бурным развитием информационных технологий и их широким применением практически во всех областях человеческой деятельности все большее внимание уделяется средствам защиты информации. Вместе с тем, как показывает анализ, в ряде случаев современные криптографические средства защиты не полностью удовлетворяют потребностям пользователей, и на первый план выдвигаются стеганографические средства, которые призваны скрыть от посторонних сам факт присутствия объекта защиты. При этом, стеганографические средства защиты, по сравнению с криптографическими, предполагают значительно больший уровень защиты, так как не провоцируют противника на активное противодействие защитным механизмам.

Вместе с тем, наиболее удобным, с точки зрения пользователя, способом хранения больших объемов данных является их структурирование в рамках файловой организации. Этим определяется присутствующий в исследованиях последних лет широкий интерес к проблемам защиты информации на уровне файловых систем (ФС) хранения данных. Однако, как показывает анализ, существующие стеганографические файловые системы (СФС), призванные обеспечить максимальный уровень защиты, не в состоянии предоставить достаточно большие объемы хранимой информации. Более того, в некоторых СФС для обеспечения относительно большого объема хранимой информации применяется специальная организация данных, в результате чего их возможности и техника использования существенно отличаются от традиционных ФС. Последнее несколько усложняет работу пользователя и тем самым ограничивает реальное применение СФС.

Наряду с созданием новых средств защиты информации, в частности СФС, не менее актуальной остается разработка адекватных методов оценки и сравнения их эффективности. Как показывает проведенный в работе анализ, существующие методы оценки стойкости стеганографических систем, отражая специфику применяемых принципов сокрытия информации, зачастую не позволяют достаточно полно сопоставлять средства защиты, имеющие различную природу и организацию обеспечения скрытности.

Широкое развитие технологий локальных и глобальных сетей делает не только возможным, но и технически целесообразным создание и применение таких распределенных в сети ФС, как CIFS (Windows), NFS (Unix) и др. Вполне естественным при этом представляется создание защищенных сетевых распределенных ФС, в частности, распространение принципов проектирования СФС на распределенные ФС.

Цель и задачи работы. Исходя из вышеизложенного, целью диссертационной работы является исследование и разработка принципов проектирования СФС, призванных обеспечить большую защищенность и объем хранимой информации и методов оценки стойкости разнородных СФС. Для достижения указанной цели в работе ставятся и решаются следующие основные задачи:

- провести анализ современного состояния и определить актуальные задачи проектирования СФС;

- исследовать и разработать принципы проектирования стеганографических средств защиты, позволяющие существенно увеличить объем скрываемой информации;
- исследовать и разработать методы оценки стойкости стеганографических систем, позволяющие предельно полно сопоставлять средства защиты, имеющие различную природу и организацию обеспечения скрытности;
- исследовать возможность и выбрать пути распространения принципов проектирования СФС на распределенные ФС в рамках локальных и глобальных сетей.

Объект исследования. Объектом исследования в работе являются принципы проектирования и реализации стеганографических файловых систем.

Методы исследования. Исследования, проводимые в работе, основаны на комплексном использовании методов криптографии, стеганографии, математического анализа, теории вероятностей, математической статистики, комбинаторного анализа и теории алгоритмов.

Научная новизна. В диссертационной работе получены и выносятся на защиту следующие научные результаты:

- разработан метод сокрытия информации посредством группировки и перестановки разнотипных контейнеров, который позволяет скрывать в два и более раза больше метаданных СФС и, следовательно, многократно больше пользовательских данных;
- предложен новый подход к построению СФС, позволяющий, наряду с увеличением объема скрываемой информации посредством использования свободных областей носителя для хранения пользовательских данных, повысить стойкость системы за счет одновременного использования разнотипных контейнеров для хранения метаданных СФС;
- предложен метод многоуровневой защиты информации в СФС, который, в отличие от существующих, обеспечивает большую скрытность данных пользователей более высоких уровней защиты, одновременно поддерживая их целостность;
- предложен новый стеганографический метод удаленной регистрации и удаленной аутентификации пользователей СФС, который, в отличие от существующих, позволяет скрыть как саму процедуру регистрации, так и последующую аутентификацию, что, в свою очередь, способствует повышению их стойкости к атакам противников;
- сформулирован метод оценки стойкости стеганографических систем, который впервые позволяет оценивать и на этой основе сравнивать средства защиты, имеющие различную природу и организацию обеспечения скрытности.

Практическая значимость результатов, полученных в диссертационной работе, заключается в следующем:

- разработана и реализована СФС с многоуровневой организацией защиты в операционной системе Linux на основе ФС ext2, которая позволила по сравнению с существующими СФС существенно увеличить объем скрываемой информации и повысить стойкость в 2,5 – 3 раза, одновременно предоставляя дополнительные функциональные возможности;

- разработаны протоколы удаленной регистрации и удаленной аутентификации пользователей СФС, обеспечивающие в типичных случаях повышение стойкости процедуры аутентификации более чем на порядок величины;
- произведено обобщение результатов опытной эксплуатации реализованной СФС, что дало возможность сформулировать практические рекомендации по построению распределенных СФС на базе локальных сетей и Интернет, позволяющие поднять на качественно новый уровень защищенность распределенных массивов данных.

Внедрение. Результаты диссертационной работы внедрены в систему защиты информации компании Altacode LLC, что подтверждено соответствующим актом.

Апробация полученных результатов. Основные результаты работы докладывались на годичных конференциях ГИУА (2005, 2006 гг.), семинарах кафедры ИБПО ГИУА (2005-2007 гг.) и Института Проблем Информатики и Автоматизации НАН РА (2007 г.), международных конференциях CSIT 2007, 2009 (Computer Science and Information Technologies), SAM07 (Security and Management 2007) и международной научно-практической конференции по вопросам безопасности информационных систем (2008 г.).

Публикации. Основные результаты работы опубликованы в 10-и научных трудах, список которых представлен в конце автореферата.

Структура и объем работы. Диссертационная работа состоит из введения, пяти глав, списка цитируемой литературы, насчитывающий 88 наименований и четырех приложений. Объем работы – 145 страниц, включающих 23 рисунка и 13 таблиц. Диссертация написана на русском языке.

## СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы, сформулированы цель работы, научная новизна, практическая значимость и основные положения, выносимые на защиту.

В первой главе определены основные термины, принятые в области стеганографии, проведен анализ существующих методов сокрытия информации и методов оценки стойкости стеганографических систем защиты информации.

В §1.1 кратко представлена стеганография, как одна из наук, занимающихся вопросами защиты информации, а также приведены ее основные отличия от криптографии.

В §1.2 представлена терминология, принятая в стеганографии и используемая в рамках данной диссертационной работы.

В §1.3 рассмотрены основные методы сокрытия информации в цифровых контейнерах. Приведены основные различия между форматными и неформатными методами сокрытия информации.

В §1.4 представлен один из наиболее известных теоретических методов оценки стойкости стеганографических систем – теоретико-информационный. Данный метод основывается на известной схеме стеганографической системы с наличием пассивного противника (рис. 1).

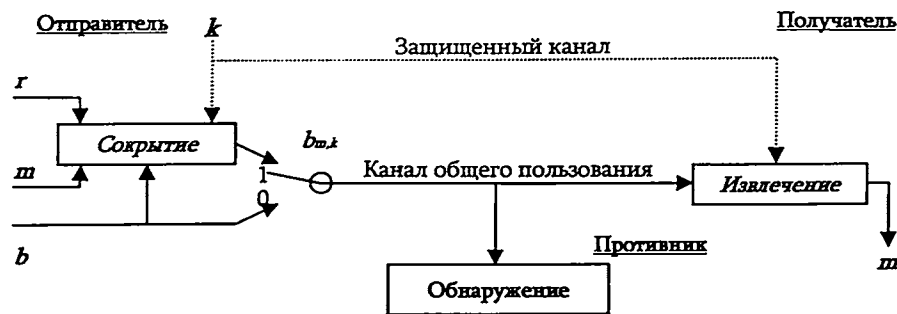


Рис. 1. Общая схема стеганографической системы с присутствием пассивного противника

Схема предполагает присутствие трех участников: отправителя, получателя и противника. Отправитель может действовать только в двух режимах либо он активен (посылает модифицированный контейнер  $b_{m,k}$ ), либо пассивен (посылает пустой контейнер  $b$ ).

Если отправитель активен, то он изменяет пустой контейнер  $b$ , скрывая в нем сообщение  $m$  с использованием секретного ключа  $k$  и секретного случайного значения  $r$  для настройки алгоритма сокрытия. В результате сокрытия он получает модифицированный контейнер  $b_{m,k}$ , который передает получателю. Получатель должен извлечь из контейнера  $b_{m,k}$  скрытое сообщение  $m$  с помощью ключа  $k$ .

Задачей противника является обнаружение факта передачи скрытого сообщения (выявление скрытого канала).

В §1.5 представлены известные теоретические абсолютно стойкие стеганографические системы, в том числе одноразовый стеганографический блокнот и протокол скрытой передачи одного бита информации. Приведены их свойства абсолютной стойкости, а также представлены их доказательства с использованием теоретико-информационного метода оценки стойкости.

В §1.6 представлены результаты исследований в области статистического стеганоанализа и методов взлома стеганографических систем. Представлены основные принципы поддержания защищенности стеганографических систем на необходимом уровне. Выявлены основные критерии обнаружения существования скрытого канала в стеганографических системах. Представлено использование статистического критерия *Chi-квадрат* в статистическом стеганоанализе.

Во второй главе приводятся стандартные подходы к организации файловых систем со стеганографической защитой информации, методы аутентификации пользователей, а также методы построения многоуровневой защиты.

В §2.1 рассмотрены известные принципы проектирования СФС и представлены существующие реализации СФС. Обоснованы и представлены недостатки этих систем, при их применении на практике. К основным недостаткам, в частности, относятся:

- недостаточная емкость сокрытия для пользовательских данных, или достаточная – но за счет понижения стойкости и защищенности системы в целом;

- низкое быстродействие, что негативно отражается на стойкости системы и целесообразности ее применения на практике;
- хранение метаданных, ключей, программ администрирования не методами стеганографии, что, негативно отражается на стойкости СФС;
- проведение аутентификации, авторизации и всех остальных шагов контроля доступа к системе посредством методов криптографии, что неприемлемо при проектировании систем скрытнописи;
- неудобство использования из-за больших требований к пользователям такой системы, или усеченного набора возможностей данной системы по сравнению с традиционными ФС.

В §2.2 представлены основные методы организации процедуры аутентификации в системах защиты информации.

В §2.3 кратко рассмотрены основные методы взлома криптографических систем защиты информации. Основные выводы позволяют нам искать решение проблемы защиты информации в сфере стеганографии:

- разработчики криптографических систем защиты информации не всегда делают правильные предположения о возможностях противника;
- пользователи криптографических систем защиты информации не всегда следуют требованиям и рекомендациям разработчиков, тем самым ставя систему под угрозу взлома.

В §2.4 представлены основные методы организации многоуровневой защиты в системах хранения и передачи информации.

В третьей главе дается описание новых методов сокрытия информации в цифровых контейнерах и представлены принципы построения стойких СФС. Приводится описание разработанной стеганографической файловой системы с многоуровневой защитой данных. Описаны основные алгоритмы, используемые при организации работы данной СФС. Представлены протоколы сетевой регистрации ключа аутентификации и удаленной аутентификации пользователя без предоставления информации о закрытом ключе.

В §3.1 приведен обобщенный метод сокрытия информации путем перестановки элементов последовательностей контейнеров. Описывается алгоритм нахождения перестановки на основе целочисленного ключа. Приводится описание обобщенного алгоритма сокрытия данных путем перестановки тех элементов контейнера, последовательность которых не важна с точки зрения стандартного обработчика.

В §3.2 приведены практические примеры использования определенного выше метода.

В §3.3 представлен метод группировки контейнеров, при использовании которого наблюдается логарифмический рост пространства сокрытия. Даны примеры его применения и представлены его основные недостатки.

В §3.4 представлен метод сокрытия информации в разнородных контейнерах путем использования ключа, определяющего последовательность выбранных контейнеров.

Приведем формальное описание метода. Зафиксируем директорию в файловой системе -  $J$ . Обозначим все файлы, находящиеся в поддиректориях  $J$  и пригодные для

сокрытия, через  $F_1, F_2, \dots, F_n$ . Их можно упорядочить по какому-либо критерию (алфавитное упорядочение, поиск дерева директорий в ширину или в глубину и т.д.).

Вышеотмеченное упорядочение  $UP = \langle F_1, F_2, \dots, F_n \rangle$  назовем *единичной перестановкой* файлов, пригодных для сокрытия, или просто - единичной перестановкой файлов-контейнеров.

*Ключевой последовательностью* метода сокрытия в разнородных контейнерах назовем последовательность  $KP = \langle F_{k1}, F_{k2}, \dots, F_{kn} \rangle$ , которая получается при перестановке элементов  $UP$  согласно фиксированному ключу  $k$ . Согласно §3.1, существует метод определения ключа и алгоритм перестановки какой-либо последовательности согласно данному ключу так, чтобы позже однозначно было возможно извлечь ключ  $k$ .

Ключевая последовательность определяет порядок выбора файлов-контейнеров. Последнее нам необходимо для последующего сокрытия информации в этих контейнерах.

Для каждого типа контейнера определим целочисленную, неотрицательную функцию емкости контейнера в виде:

$$I_{\max}(F) = g_t(F),$$

где  $t$  - тип контейнера (напр., *bmp, gif, wav, mp3, doc* и т.д.), а  $F$  - конкретный файл-контейнер.

Другими словами, для каждого контейнера нас интересует его емкость сокрытия, которая задается функцией  $g_t$ .

Обозначим скрываемое сообщение через  $m$ . Также предположим, что  $m$  представляется в виде бинарной последовательности (что всегда возможно, так как мы имеем дело с цифровой стеганографией и, следовательно, с цифровым представлением информации). Разобьем  $m$  последовательно на куски таким образом, чтобы

$$m = \bigoplus_{i=1}^n m_i,$$

где бинарная операция  $\bigoplus$  представляет собой процедуру дописывания бинарной последовательности второго аргумента в конец бинарной последовательности первого аргумента (другими словами - конкатенация бинарных последовательностей). Мы будем также требовать, чтобы после разбиения сообщения  $m$  имело место следующее отношение:

$$I(m_i) = g_{t_i}(F_i).$$

Если такое разбиение существует, то сообщение  $M$  возможно скрыть в группе файлов-контейнеров  $F_i$ . Проблема  $\sum I(m_i) < \sum g_{t_i}(F_i)$  решается одним из нижеперечисленных известных методов:

- в конец сообщения  $m$  дописываются недостающие данные в виде заранее определенной последовательности;
- в начало сообщения  $m$  добавляется заголовок, где указывается общая длина сообщения  $m$ .

Предположим, что для каждого типа ( $t_i$ ) контейнера существует несколько методов сокрытия ( $q_i$ ). Для того, чтобы было возможно извлечь данные из контейнеров, необходимо иметь информацию о методе, используемом при сокрытии в каждом из

контейнеров. Для этого, в данной работе, предлагается включить эту информацию в стеганографический ключ. В рамках данной работы был выбран второй метод. Итак, закрытый стеганографический ключ для данного метода сокрытия данных в разнородных контейнерах имеет структуру, изображенную на рис. 2.

Кол-во контейнеров	Дистанция от UP	Директория J	$q_{t_1}$	$q_{t_2}$	$q_{t_i}$	$q_{t_n}$
--------------------	-----------------	--------------	-----------	-----------	-----------	-----------

Рис. 2. Структура закрытого ключа

Максимальная емкость сокрытия данным методом вычисляется по следующей формуле:

$$I_{\max} = \sum_{i=1}^n I_{\max}(F_i, q_i).$$

Далее приводятся три основных случая применения данного метода:

- увеличение пространства сокрытия;
- использование разнотипных контейнеров;
- поддержание необходимого уровня стойкости.

В §3.5 представлен принцип проектирования СФС, при котором делается разграничение между метаданными и пользовательскими данными. Метаданные скрываются методом сокрытия в разнородных контейнерах, представленным в §3.4, а пользовательские данные скрываются в свободных кластерах оригинальной файловой системы.

Такой подход дает возможность одновременно защитить метаданные от активных атак противников, повысить емкость сокрытия пользовательских данных и стойкость к атакам пассивных противников.

В §3.6, с целью обеспечения надежной защиты и одновременно предоставления механизма стеганографической аутентификации, предлагается использовать метод, основанный на поведении (последовательности действий) пользователя в рамках ФС.

Обозначим операции ввода/вывода/администрирования ФС (далее - операция) через  $g_i(a_{i1}, a_{i2}, \dots, a_{in})$ , где  $a_{ij}$  -  $j$ -й параметр  $i$ -й операции ФС. Также определим две особые операции. Первую операцию обозначим через  $g^*$ . Она не имеет параметров и представляет собой конечную последовательность любой из операций  $g_i(a_{i1}, a_{i2}, \dots, a_{in})$ . Вторую операцию обозначим через  $g^m$ . Она также не имеет параметров и представляет собой последовательность из любых  $m$  операций  $g_i(a_{i1}, a_{i2}, \dots, a_{in})$ .

*Закрытым стеганографическим ключом аутентификации* пользователя СФС назовем следующую последовательность:

$$G = \langle g_{t_1}(a_{t_1,1}, a_{t_1,2}, \dots, a_{t_1,n_1}), g_{t_2}(a_{t_2,1}, a_{t_2,2}, \dots, a_{t_2,n_2}), \dots, g_{t_i}(a_{t_i,1}, a_{t_i,2}, \dots, a_{t_i,n_i}) \rangle.$$

При использовании стеганографической системы *моментом аутентификации* пользователя назовем тот момент времени, когда пользователь произвел последовательность действий, которые задаются ключом  $G$ .

После прохождения аутентификации ФС должна предоставлять аутентифицированному пользователю скрытые объекты файловой системы соответствующего уровня защиты. При такой организации механизма аутентификации необходимо привести систему в начальное состояние. Например, если в результате процесса аутентификации пользователь, согласно своему ключу  $G$ , создал две директории, три файла и один файл удалил, то после удачной аутентификации все эти промежуточные файловые объекты следует удалить, а все удаленные объекты - восстановить. Вся процедура приведения системы аутентификации в начальное состояние может производиться файловой системой сразу после удачной аутентификации.

Далее оценивается стойкость данного метода к атакам эвристического перебора ключей и к атакам типа "перепроигрывание" и "человек посередине". В первом случае получаем на порядок превышающую стойкость по сравнению с известными криптографическими системами с открытым ключом. Во-втором случае доказывается невозможность перепроигрывания протокола противником.

В §3.7 представлен протокол идентификации с нулевым разглашением, основанный на проблеме нахождения дискретного логарифма. Суть идеи состоит в том, чтобы предъявить всего лишь один бит информации – факт того, что претендент знает секрет.

Цель протокола состоит в том, чтобы сторона  $A$  доказала знание секрета  $s$  (которое связано с общеизвестными истинными данными) любому верификатору  $B$ , не раскрывая никакой информации о  $s$ , неизвестном и невычислимом стороной  $B$  до начала работы протокола. Стойкость протокола основывается на сложности нахождения дискретного логарифма, принадлежащего к мультипликативной группе  $Z_p^*$ , где  $p$  – простое число.

В §3.8 представлены два протокола – протокол удаленной регистрации стеганографического ключа аутентификации и протокол удаленной аутентификации пользователя СФС. В качестве доказательства подлинности пользователя в первом протоколе выбран протокол идентификации с нулевым разглашением, представленный в §3.7. Второй протокол является упрощенным вариантом первого – без фазы идентификации с нулевым разглашением. Схема работы протокола удаленной регистрации стеганографического ключа аутентификации представлена на рис. 4.

В §3.9 представлен метод организации многоуровневой защиты СФС, который, во-первых, повышает защищенность системы от взломов и, во-вторых, позволяет автоматически удалять данные пользователей с истекшим сроком регистрации в системе.

Для повышения уровня защиты данных пользователей более высоких уровней защиты в данной работе предлагается использовать нижеприведенный подход. Так как основным способом обнаружить и получить доступ к пользовательским данным является обнаружение метаданных, то попробуем защитить метаданные более эффективным способом.

Назовем пользовательскими данными *нулевого уровня* защиты совокупность всех стеганографических контейнеров, полученных при поиске в глубину директории  $J$  (см. §3.4), как место для хранения метаданных методом сокрытия в разнородных контейнерах.

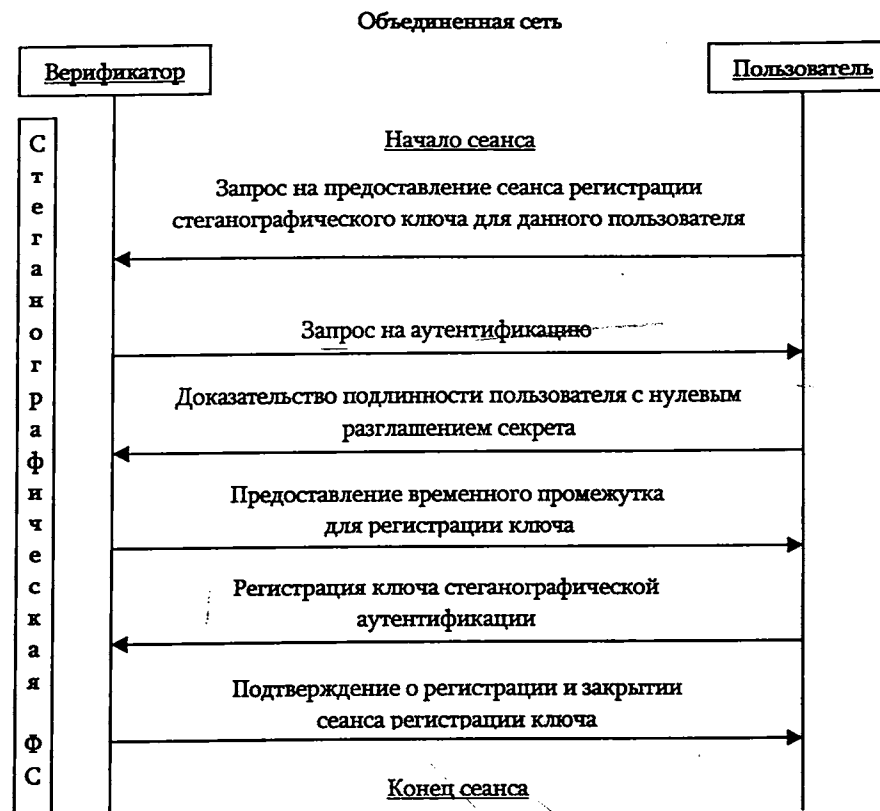


Рис. 4. Схема работы протокола удаленной регистрации стеганографического ключа аутентификации

Заметим, что пользовательские данные нулевого уровня защиты доступны всем пользователям ФС – они вообще не скрыты. Реальная стеганографическая защита применяется начиная с первого уровня. Отметим, что в СФС, на каждый момент времени, существует  $L$  реальных уровней защиты (естественно, не считая нулевого уровня защиты).

При сокрытии метаданных пользователя уровня защиты  $i$  ( $1 \leq i \leq L$ ), будем использовать пользовательские данные из уровней защиты от 0 до  $(i-1)$ . Например, метаданные пользователя второго уровня скрываются в обычных, незащищенных файлах оригинальной ФС и в скрытых пользовательских данных СФС первого уровня защиты. При такой структуре сокрытия противнику придется взломать  $i-1$  более низких уровней защиты, для того, чтобы получить доступ к данным пользователя уровня  $i$ . Очевидно, что такая структура существенно повышает стойкость СФС и дает еще больше возможностей избежать обнаружения пользовательских данных более высоких уровней защиты. Существенный рост защищенности пользовательских данных высоких уровней

достигается за счет применения более сложных алгоритмов, используемых при проектировании СФС. СФС ответственна за организацию скрытия таким образом, чтобы метаданные разных пользователей не перекрывались, так как это приведет к уничтожению части метаданных. Разработанная в рамках данной работы СФС решает эти задачи предоставляя чуть более усложненный вариант метода сокрытия в разнородных контейнерах.

§3.10 рассмотрены возможности расширения разработанной СФС до распределенной СФС.

Основной задачей распределенной СФС является предоставление пользователю возможности использования распределенных, в вычислительной сети, файлов, не замечая факта удаленности объектов файловой системы. Дополнительными требованиями являются синхронизация и контроль доступа к файлам и директориям, а также обнаружение и исправление ошибок при передаче данных по сети. В случае стеганографических файловых систем, к распределенной СФС добавляются следующие требования:

1. сокрытие метаданных в распределенной сети;
2. сокрытие пользовательских данных в распределенной сети;
3. сокрытие факта передачи защищенных данных по каналам передачи вычислительной сети;
4. сокрытие факта прохождения процедуры аутентификации в сети;
5. сокрытие удаленной регистрации стеганографических ключей.

В результате наблюдается существенное повышение защищенности пользовательских данных, за счет их распределения по многим станциям вычислительной сети, что на порядок усложняет процедуру поиска и группирования необходимых контейнеров, содержащих отрезки защищенной информации.

В четвертой главе представлены два новых метода оценки стойкости, дающие возможность сравнивать разнородные стеганографические системы.

В §4.1 рассмотрены основные недостатки теоретико-информационного метода оценки стойкости, приведенного в §1.4. Доказана невозможность использования данного метода при оценке стойкости разнородных систем и его применения на практике.

Часто пользователю требуется оценить стойкость нескольких разнотипных методов сокрытия, чтобы сделать обоснованный выбор в пользу одного из них. Например, пользователю необходимо решить, использовать метод сокрытия в графическом контейнере или в музыкальном файле *mp3*. При этом его интересует только стойкость метода – ему безразлично, куда прятать свои данные. Ясно, что теоретико-информационный метод оценки стойкости не дает ему возможности сделать выбор, так как значения стойкости, вычисленные данным методом, неоднородны для разнотипных методов сокрытия. Лишь в случае абсолютно стойких стеганографических систем можно утверждать о том, что они одинаково стойки к атакам пассивных противников.

В §4.2 представлен новый теоретический метод оценки стойкости разнородных стеганографических систем. Он построен на основе известной схемы стеганографической системы с присутствием пассивного противника, представленной на рис. 1.

Начнем с простого случая. Предположим, что по каналу общего пользования могут отсылаться контейнеры одного типа  $K$  и для этого типа контейнеров существует единственный параметр  $T$ , который имеет известное (в частности – известное всем трем участникам в нашей модели) среднестатистическое распределение значений:

$$Y = \langle Y_1, Y_2, \dots, Y_k \rangle,$$

где  $k$  – это количество категорий для параметра  $T$ . Случайным событием назовем определение значения параметра  $T$  противником и, соответственно, определение принадлежности к одной из  $k$  категорий. Ясно, что для  $Y$  имеют место аксиомы Колмогорова. Противник, анализируя статистическую характеристику параметра  $T$  в контейнере, решает что либо он содержит скрытые данные, либо он пуст. Предполагается, что противник будет использовать множество статистических критериев, для оценки отклонений закономерностей в значениях параметра  $T$  для анализируемого контейнера. В настоящей работе предлагается использовать критерий *Хи-квадрат* для оценки стойкости стеганографической системы против атак пассивного противника, основываясь на следующих утверждениях:

- это один из самых известных статистических критериев;
- он успешно используется при анализе систем скрытнописи для выявления скрытого канала (см. §1.6);
- данный критерий является основным методом проверки нарушения закономерностей, используемым в сочетании с другими методами;
- критерий предполагает использование конечного числа категорий, что делает его использование на практике более предпочтительным, в отличие от непрерывных критериев, предполагающих бесконечное множество категорий;
- он основан на общем принципе наименьших квадратов, что опять-таки делает его более предпочтительным с точки зрения применения на практике.

*Стойкость* представленной стеганографической системы к атакам пассивных противников является значение дистанции *Хи-квадрат* между ожидаемым и наблюдаемым распределениями вероятностей параметра  $T$ :

$$V = \sum_{s=1}^k \frac{(Y_s - np_s)^2}{np_s},$$

где  $Y_s$  – это наблюдаемое число попаданий значения параметра  $T$  в категорию  $s$ ,  $p_s$  – ожидаемая вероятность попадания значения параметра  $T$  в категорию  $s$ ,  $l$  – количество проведенных экспериментов.

В §4.3 приводятся основные свойства разработанного критерия оценки стойкости стеганографических систем. Доказывается, что данный критерий сохраняет свойство абсолютной стойкости систем, абсолютно стойких согласно теоретико-информационному методу.

В §4.4 введен формализм, на основе клеточных автоматов, для определения понятия защищенности стеганографической системы. Даются определения *абсолютно защищенных, статистически защищенных и вычислительно защищенных* стеганографических систем.

В §4.5 представлен практический метод оценки стойкости стеганографических систем, основанный на теоретическом методе, описанном в §4.2. В отличие от теоретического метода он дает возможность оценивать и сравнивать реальные стеганографические системы и к тому же наследует свойство, дающее возможность сравнивать разнородные системы.

Допустим, что для стеганографической системы  $\Psi$  существует множество параметров

$$T = \{T_1, T_2, \dots, T_m\},$$

которые могут быть проанализированы противником на предмет выявления отклонений распределения их значений от ожидаемых значений. Целью разработчика системы является:

- выявление всех тех параметров, которые имеют существенные отклонения от среднестатистических значений при создании скрытого канала;
- разработка методов сокрытия, при которых у противника, при известном статистическом анализе контейнера, не появится серьезных оснований для предположения о существовании скрытого канала в системе.

Итак, предположим, что параметр  $T_i$ , как случайная величина, имеет функцию плотности распределения  $f(T_i)$ . Разобьем интервал  $(-\infty, +\infty)$  на  $k$  частей

$$(-\infty, a_{i1}), (a_{i1}, a_{i2}), \dots, (a_{i,k-1}, +\infty)$$

таким образом, чтобы имели место следующие равенства:

$$\int_{-\infty}^{a_{i1}} f(T_i) = \int_{a_{i1}}^{a_{i2}} f(T_i) = \dots = \int_{a_{i,k-1}}^{+\infty} f(T_i) = \frac{1}{k}$$

Для того чтобы получить оценку, которая будет учитывать все параметры  $T_i$ , будем следовать очевидной логике – просуммируем взвешенные значения стойкости по всем параметрам, т.е.:

$$V = \sum_{i=1}^m \lambda_i \left( \frac{k_i}{n} \sum_{s=1}^{k_i} (Y_{i,s})^2 - n_i \right). \quad (1)$$

Учитывая следующие зависимости между коэффициентами  $\lambda_i$ :

$$\lambda_i \geq 0 \quad \text{и} \quad \sum_{i=1}^m \lambda_i = m$$

и подставляя в (1), получим конечный вид формулы оценки стойкости для сложных и разнородных систем скрытнописи:

$$V = \sum_{i=1}^m \lambda_i \frac{k_i}{n_i} \sum_{s=1}^{k_i} (Y_{i,s})^2 - \sum_{i=1}^m \lambda_i n_i.$$

В §4.6 даны рекомендации по применению практического метода оценки, приведенного в §4.4, и примеры оценки и сравнения стеганографических систем данным методом.

В §4.7 даны практические соображения, на основе известных результатов, по оценке стойкости интерактивных систем скрытнописи. Представлены основные

параметры компьютерных систем, на основе которых можно применить предложенную выше оценку стойкости.

В пятой главе описывается программная реализация драйвера стеганографической файловой системы. Представлены результаты сравнения и тестирования разработанной СФС и существующих систем. В рамках данной главы приведена оценка стойкости разработанной стеганографической файловой системы *FS\_Stegano* методом, приведенным в §4.7.

В §5.1 описывается структура драйвера, его реализация и внедрение в операционную систему *Linux* версии ядра 2.4. Представляются ключевые структуры данных на языке *C*, которые являются основой в разработанном драйвере ФС. Приводится описание взаимодействия кода драйвера СФС с оригинальным кодом драйвера *ext2*. Оценивается объем метаданных, скрывающихся в обычных файлах.

В §5.2 задаются параметры системы, на основе которой проводились тесты, и ограничения, которые предполагались при тестировании СФС. Проведены 2 основных теста: тест на использование памяти и тест на быстродействие. Результаты приведены в виде графиков зависимостей.

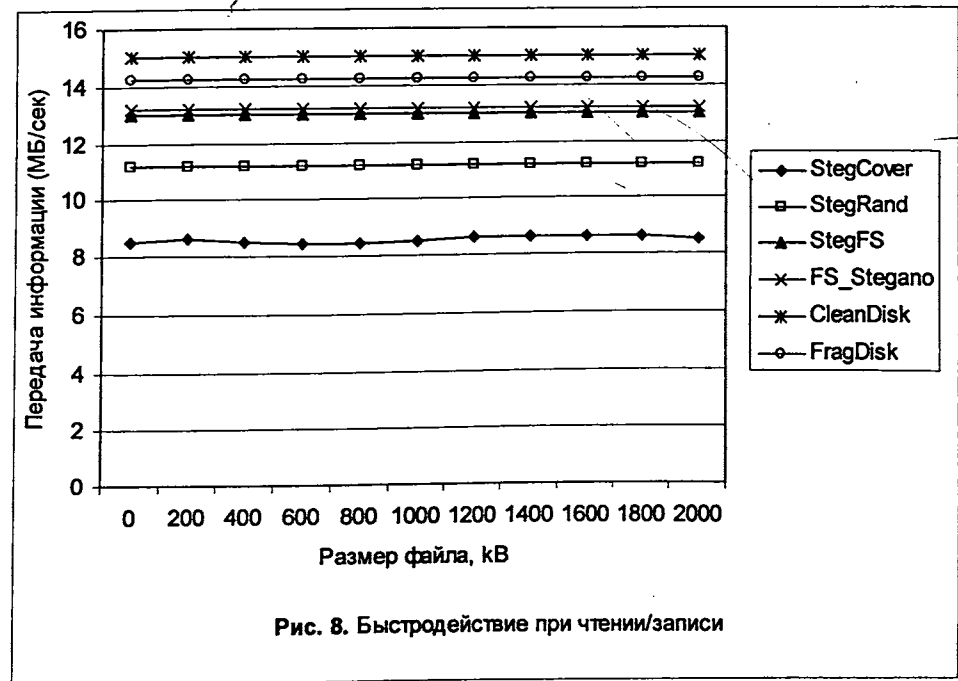
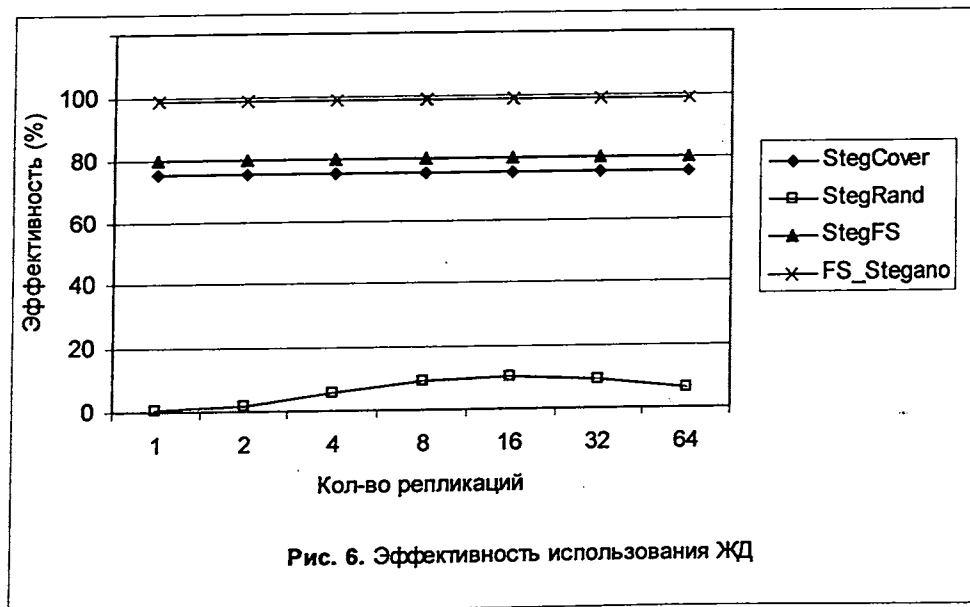
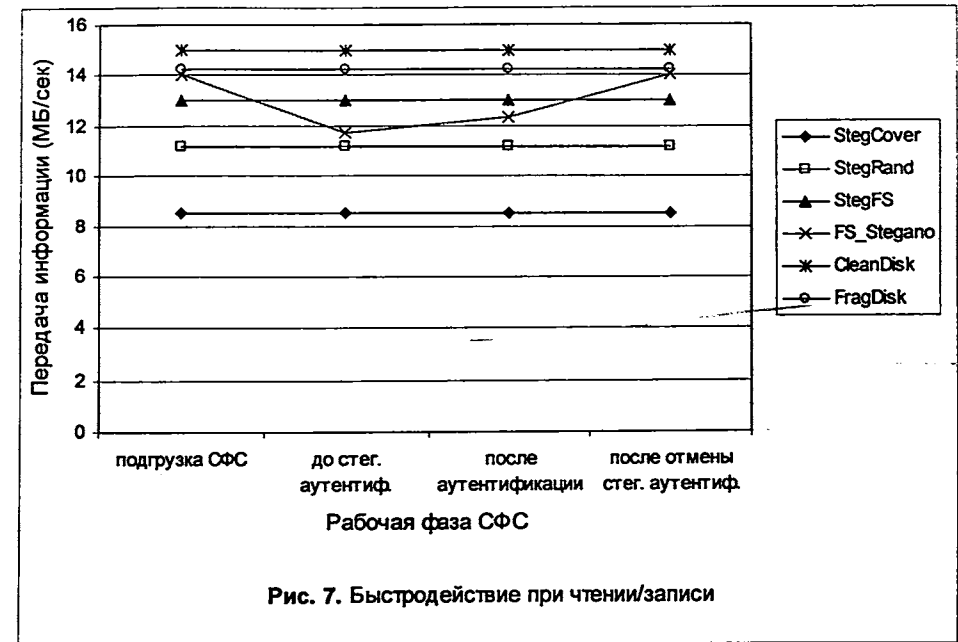
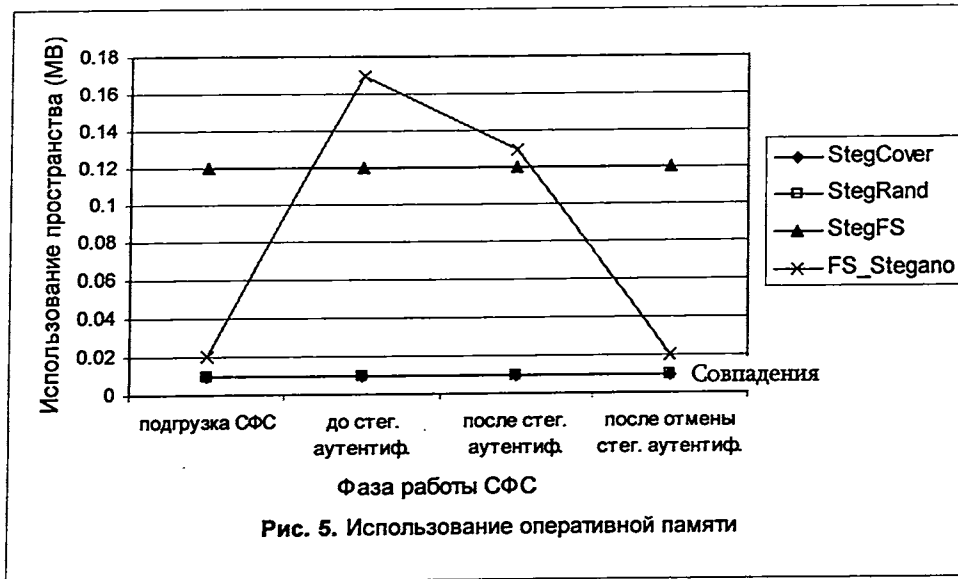
В §5.3 представлены результаты тестирования использования памяти разработанным драйвером. На рис. 5 представлена зависимость использования оперативной памяти от фазы работы СФС. Резкий пик в случае *FS\_Stegano* объясняется тем фактором, что СФС контролирует поведение пользователя по его файловым действиям (см. §3.6), что требует построения и прогона конечного автомата в памяти для обнаружения прохождения процедуры стеганографической аутентификации. Сразу после прохождения этой процедуры, либо после истечения дозволенного срока регистрации СФС удаляет данные, необходимые для организации стеганографической аутентификации и более не следит за поведением пользователя.

На рис. 6 представлен график эффективного использования пространства жесткого диска. Чем более эффективно использование, тем больше информации мы можем скрыть с меньшим количеством потерь пространства из-за присутствия метаданных (*FS\_Stegano*, *StegFS*) или покинутых блоков данных (*StegFS*).

В §5.4 приведены результаты тестирования быстродействия разработанного драйвера СФС. На рис. 7 представлены значения быстродействия в разных фазах работы СФС. Реализация файловой системы обеспечивает минимальные отклонения от быстродействия оригинальной ФС после истечения дозволенного срока и отмены аутентификации. На рис. 8 представлена зависимость быстродействия от размера скрытых файлов. Так как файлы в тестовой конфигурации небольшие (< 2МБ), заметных отклонений при увеличении размера файлов не наблюдается.

В §5.5 представлена программа администрирования. Под администрированием СФС *FS\_Stegano* понимаем набор действий, направленный на изменение метаданных СФС. Потребность в администрировании диктуется необходимостью время от времени подправлять и обновлять определенные части метаданных. В рамках данной работы была разработана программа для администрирования представленной СФС. Предполагается, что она должна быть доступна только суперпользователю. Предлагается хранить данную

программу либо на съемном диске, либо в СФС на самом привилегированном уровне защиты.



## ПЕРЕЧЕНЬ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИОННОЙ РАБОТЫ

В §5.6 приведена оценка стойкости СФС *FS\_Stegano* и двух известных СФС - *StegCover* и *StegFS* практическим методом оценки стойкости, представленным нами в главе 4. Полученные значения стойкости показывают, что разработанная СФС имеет стойкость от 2.5 до 3 раз превышающую стойкость самых известных и распространенных СФС.

В заключении перечислены основные результаты работы.

В приложении 1 приведена ключевая часть исходного кода реализации драйвера СФС *FS\_Stegano*.

В приложении 2 приведен исходный код программного инструмента для вычисления стойкости стеганографических систем по разработанному методу.

В приложении 3 приведено решение государственного комитета по языку РА о регистрации термина "стеганография".

В приложении 4 приведен акт внедрения СФС *FS\_Stegano* в подсистему защиты и хранения данных компании Altacode LLC.

## ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

1. Разработан метод сокрытия информации, основанный на группировке и перестановке разнотипных контейнеров, который позволяет скрывать в несколько раз больше метаданных СФС, в результате чего существенно повышается объем сокрытия пользовательских данных [4].
2. Предложен новый подход к построению СФС, который позволяет значительно увеличить объем скрываемой информации посредством использования свободных областей носителя, одновременно повышая стойкость системы за счет совместного использования разнотипных контейнеров для хранения метаданных СФС [2, 3, 4].
3. Предложен метод многоуровневой защиты информации в СФС, который, в отличие от существующих, обеспечивает большую скрытность данных пользователей более высоких уровней защиты, одновременно поддерживая их целостность [6].
4. Предложен новый стеганографический метод и разработаны протоколы удаленной регистрации и удаленной аутентификации пользователей СФС, которые, в отличие от существующих, позволяют скрыть как саму процедуру регистрации, так и последующую аутентификацию, что обеспечивает повышение стойкости последней более чем на порядок величины [6, 7, 8, 9].
5. Разработана и реализована СФС с многоуровневой организацией защиты в операционной системе Linux на основе ФС ext2, которая позволила по сравнению с существующими СФС существенно увеличить объем скрываемой информации и повысить стойкость в 2,5 – 3 раза, одновременно предоставляя дополнительные функциональные возможности [3, 4].
6. Разработан метод оценки стойкости стеганографических систем, который впервые позволяет оценивать и на этой основе сравнивать разнотипные стеганографические средства защиты [1, 5, 10].
7. Сформулированы практические рекомендации по построению распределенных СФС, позволяющие поднять на качественно новый уровень защищенность распределенных массивов данных [4, 6].

1. Маргаров Г., Казарян А., Обоснованное принятие решений при проектировании системы скрытнописи // Сборник материалов годичной конференции ГИУА. –Ереван, 2005. –Т. 2. –С. 497-500.
2. Ղազարյան Հ., Ինֆորմացիայի բարևարումը բազմաթյունների հաշտորդականությունների ձևափոխման հիման վրա // ՀԳՃՀ տարեկան գիտաժողովի նյութերի ժողովածու. –Երևան, 2005. –Հ. 2. –Էջ. 500-502:
3. Казарян А., Два подхода к организации стеганографической файловой системы // Сборник материалов годичной конференции ГИУА. –Ереван, 2006. –Т. 1. –С. 389-392.
4. Ghazaryan H., Steganographic file system development based on the information hiding scheme by permutation of sequence elements // Proceedings of the 2007 International Conference on Security and Management. –Las Vegas Nevada, USA, -2007. –P 107-111.
5. Казарян А., Оценка стойкости стеганографических систем на модели с наличием пассивного противника // Вестник ГИУА. Серия "Моделирование, оптимизация, управление". –Ереван, 2007. –Вып. 10, -т. 1. -С. 60-65.
6. Казарян А., Построение стеганографической файловой системы с поведенческой моделью авторизации пользователя и многоуровневой защитой данных // Вестник Инженерной академии Армении. –Ереван, 2007. –Т. 4, № 2. –С. 304-308.
7. Казарян А., Организация аутентификации и авторизации в системах скрытнописи // Информационные Технологии и Управление. –Ереван, 2007. № 5, –С. 27-30.
8. Hovhannisyan S., Ghazaryan H., DLP zero-knowledge identification protocol // Proceedings of the Computer Science and Information Technologies Conference. –Yerevan, 2007. –P. 321-322.
9. Hovhannisyan S., Ghazaryan H., Generalized DLP zero-knowledge identification protocol // Доклады международной научно-практической конференции по вопросам безопасности информационных систем.–Ереван, 2008. –С. 59-61.
10. Казарян А., Оценка стойкости разнотипных стеганографических систем // Proceedings of the Computer Science and Information Technologies Conference. –Yerevan, 2009. –P. 133-136.

## ԱՄՓՈՓԱԳԻՐ

Ատենախոսական աշխատանքը նվիրված է պահպանվող ինֆորմացիայի առավել մեծ պաշտպանվածության և ծավալի ապահովմանը կոչված թաքնագրային ֆայլային համակարգերի (ԹՖՀ) նախագծման սկզբունքների և տարաբնույթ ԹՖՀ-երի կայունության գնահատման մեթոդների հետազոտմանը և մշակմանը:

Աշխատանքի հիմնական արդյունքները հետևյալն են՝

1. մշակվել է տեղեկատվության թաքցման մեթոդ՝ հիմնված տարատեսակ կոնտեյնիւրների խմբավորման և տեղափոխման վրա, որը թույլ է տալիս թաքցնել մի քանի անգամ ավելի շատ ԹՖՀ-ի մետատվյալներ, որի արդյունքում էապես աճում է օգտագործողի տվյալների թաքցման ծավալը [4];
2. առաջարկվել է ԹՖՀ-երի կառուցման նոր մոտեցում, որը թույլ է տալիս կրիչի ազատ տիրույթների օգտագործման միջոցով զգալիորեն ավելացնել թաքցվող տեղեկատվության ծավալը, միաժամանակ մեծացնելով համակարգի կայունությունը՝ ԹՖՀ-ի մետատվյալների պահպանման նպատակով տարատեսակ կոնտեյնիւրների համատեղ օգտագործման հաշվին [2, 3, 4];
3. առաջարկվել է ԹՖՀ-երում տեղեկատվության բազմամակարդակ պաշտպանության մեթոդ, որը, ի տարբերություն գոյություն ունեցողների, ապահովում է ավելի բարձր պաշտպանության մակարդակի օգտագործողների տվյալների ավելի բարձր գաղտնիություն՝ միաժամանակ պահպանելով դրանց ամբողջականությունը [6];
4. առաջարկվել է նոր թաքնագրային մեթոդ և մշակվել են հեռահար զրանցման և հեռահար նույնացման արձանագրություններ ԹՖՀ-ի օգտագործողների համար, որոնք, ի տարբերություն գոյություն ունեցողների, թույլ են տալիս թաքցնել ինչպես զրանցման գործընթացը, այնպես էլ հետագա նույնացումը, ինչը ապահովում է վերջինիս կայունության ավելի քան մեկ կարգով բարձրացում [6, 7, 8, 9];
5. մշակվել և իրագործվել է բազմամակարդակ պաշտպանության կազմակերպմամբ ԹՖՀ Linux օպերացիոն համակարգում ext2 ֆայլային համակարգի հիման վրա, որը թույլ է տվել գոյություն ունեցող ԹՖՀ-երի հետ համեմատ զգալիորեն ավելացնել թաքցվող տեղեկատվության ծավալը և բարձրացնել կայունությունը 2,5-3 անգամ, միաժամանակ տրամադրով լրացուցիչ ֆունկցիոնալ հնարավորություններ [3, 4];
6. մշակվել է թաքնագրային համակարգերի կայունության գնահատման մեթոդ, որն առաջին անգամ թույլ է տալիս գնահատել և դրա հիման վրա համեմատել պաշտպանության տարատեսակ թաքնագրային միջոցներ [1, 5, 10];
7. ձևակերպվել են բաշխված ԹՖՀ-երի կառուցման կիրառական առաջարկներ, որոնք թույլ են տալիս նոր որակական մակարդակ բարձրացնել բաշխված տվյալների գանգվածների պաշտպանվածությունը [4, 6]:

Hayk L. GHAZARYAN

“Research and development of steganographic file systems design principles and security estimation methods”