5. Создание набора прав пользователей.

6. Другие функции, которые являются опциональными, например, запись с микрофонов, кейлогер, снимки экранов пользователей, отчётности (например, выявление лояльности сотрудника), поддержка анализа на нескольких языках, модули для распознавания графики [3].

Анализ показывает, что интеграция этих систем увеличивает информационную безопасность предприятия [4]. Несмотря на то, что внешне всё выглядит готовым к интеграции, необходимо рассмотреть их совместную работу по классификации данных и обновлению, и дополнению баз, которые имеются у этих систем для стабильной совместной работы. Чтобы обеспечить стабильную работу такой системы, офицером по информационной безопасности должна регулярно проводиться работа по сопоставлению политик DLP и IRM, а значит, что такая функция должна быть доступна в такой системе. Конкретные действия офицера по ИБ, для поддержания актуальности политик:

1. Выбор для сопоставления двух подходящих друг для друга политик со стороны DLP и со стороны IRM.
2. Синхронизация политик DLP- или IRM-системы.
3. Сканирование специально встроенной программой в DLP-систему всех изменений и как следствие происходит взаимное дополнения за счёт выставленного заранее сопоставления политик.

Проанализировав все функции и методы работы DLP и IRM-систем, нельзя не прийти к заключению о необходимости их совместного применения как решения в сфере информационной безопасности на конкретном предприятии. Стоит отметить, что данный вид решения позволяет нам выйти на новую ступень в сфере защиты информации.

Интеграция этих систем в одно комплексное решение это весьма затратная процедура для малого и среднего бизнеса, поэтому разумнее будет использовать такое решение в рамках большой организации, которой действительно необходим такой уровень защиты. Однако здесь играет роль не столько денежный, сколько технический фактор. Ведь нельзя забывать про то, что некоторые системы потребляют довольно большое количество ресурсов.

**Список использованной литературы:**

1. Профилактика утечек данных: DLP, IRM и стандартные средства WS2008. — URL: https://xakep.ru (дата обращения: 28.11.15).
2. Защита информации от утечек: интеграция IRM- и DLP-решений. — URL: http://www.leta.ru (дата обращения: 28.11.15).
3. Совместное использование политик DLP и IRM в GTB DLP Suite. — URL: http://www.anti-malware.ru (дата обращения: 18.03.16).
4. Цветкова О.Л., Айдинян А.Р. Интеллектуальная система оценки информационной безопасности предприятия от внутренних угроз. — Вестник компьютерных и информационных технологий, 2014. — № 8 (122). — С. 48–53.

© Черняков П.В., 2016

**УДК 004.056**

**Шемет Владислав Сергевич**
студент ДГТУ,
**Айдинян Андрей Размикович**
к.т.н., доцент ДГТУ,
Донской государственный технический университет (ДГТУ), г. Ростов-на-Дону, РФ
E-mail: barni1993@list.ru

## ОБЗОР МЕТОДОВ ШИФРОВАНИЯ

**Аннотация**

В данной статье рассмотрены наиболее известные методы шифрования и дается их сравнительный

анализ.

**Ключевые слова**

Шифрование, стойкость шифра, методы шифрования

В наше время общество становится информационно-обусловленным, успех любого вида деятельности все сильней зависит от знания какой-либо ценной информации и от отсутствия ее у конкурентов. Поэтому особое внимание уделяется защите информации.

Современным методом защиты информации является ее шифрование. Шифрование — преобразование информации с помощью ключа в не воспринимаемый формат в целях скрытия от злоумышленников и понятный для пользователя, которому она предназначена [1]. Шифрование позволяет защититься от следующих рисков информационной безопасности: кража, раскрытие информации, подделка под оригинал. Разработано множество методов шифрования [2].

При сравнительном анализе алгоритмов шифрования необходимо учитывать следующие характеристики:

— практическую стойкость шифра;

— ресурсоемкость и энергоемкость;

— скорость работы.

Алгоритмы шифрования построены таким образом, что для вскрытия требуется перебор по ключевому пространству, поэтому стойкость шифра определяется длиной ключа.

Существует два класса методов шифрования: симметричный и асимметричный. В первом случае, как получатель, так и отправитель информации используют один ключ шифрования. Во втором же у отправителя закрытый ключ шифрования, а у получателя — открытый ключ для расшифровки.

В случае симметричной схемы шифрования каждый из субъектов каким-то образом должен доставить свои ключи всем остальным участникам обмена, при этом суммарное число используемых ключей будет достаточно велико при большом количестве участников обмена. Применение асимметричного алгоритма требует лишь рассылки открытых ключей всеми участниками, суммарное число ключей равно количеству участников обмена. На практике общедоступные ключи могут помещаться в специальную базу данных. При необходимости послать партнеру зашифрованное сообщение можно сделать сначала запрос его открытого ключа. Получив его, можно запустить программу шифрования, а результат ее работы послать адресату. На использовании общедоступных ключей базируется и так называемая электронная подпись, которая позволяет однозначно идентифицировать отправителя. Сходные средства могут применяться для предотвращения внесения каких-либо корректив в сообщение на пути от отправителя к получателю.

К симметричным методам шифрования относят следующие алгоритмы: Blowfish, DES, 3DES, CAST, AES, ГОСТ. К ассиметричным относят: RSA, El-Gamal.

Алгоритм шифрования **Blowfish** основан в 1993 году Брюсом Шнаером. В общем случае алгоритм состоит из двух этапов — расширение ключа и шифрация/дешифрация исходных данных. Сложная схема выработки ключа сильно усложняет атаку на алгоритм, если пытаться взломать её методом перебора, однако делает его непригодным для использования в системах, где ключ часто меняется, и на каждом ключе шифруется небольшие по объему данные. Алгоритм лучше всего подходит для систем, в которых на одном и том же ключе шифруются большие массивы данных.

Алгоритм шифрования **DES** основан в 1975 году фирмой IBM. С 1977 по 2001 г. являлся Федеральным стандартом шифрования США. Симметричный алгоритм шифрования, в котором используется один ключ, как для получателя, так и для отправителя, то есть этот ключ используется как для расшифрования, так и для шифрования. DES имеет блоки по 64 бит и 16 цикловую структуру сети Фейстеля, для шифрования использует ключ с длиной 56 бит. Алгоритм использует комбинацию нелинейных S-блоки и линейных преобразований. Основной недостаток — размер ключа всего 56 бит, что недостаточно для современного уровня развития компьютеров.

Алгоритм шифрования **Triple DES (3DES)** — симметричный блочный шифр, созданный в 1978 году

на основе алгоритма DES, с целью устранения главного недостатка последнего — малой длины ключа (56 бит), который может быть взломан методом полного перебора. Скорость работы 3DES в 3 раза ниже, чем у DES, но криптостойкость намного выше. 3DES является простым способом устранения недостатков DES [3].

Алгоритм шифрования **CAST** является в некотором смысле аналогом DES. В основе этого алгоритма лежит шесть S блоков с 8-битовым входом и 32-битовым выходом. Алгоритм сложный и зависит от реализации. Главной особенностью алгоритма CAST является то, что блоки не фиксируются. Используются ключи 128 и 256 бит.

Алгоритм шифрования **AES (Rijndael)** разработан в 1997 году и на данный момент является Федеральным стандартом шифрования США. В основе этого алгоритма лежит симметричный блочный шифр который работает с блоками данных длиной 128 бит и использует ключи длиной 128, 192 и 256 бит. Алгоритм может работать и с другими длинами блоков и ключей, но они в стандарт не вошли. Для шифрования в алгоритме AES применяются следующие процедуры преобразования данных: ExpandKey — вычисление раундных ключей для всех раундов; SubBytes — подстановка байтов с помощью таблицы подстановок; ShiftRows — циклический сдвиг строк в форме на различные величины; MixColumns — смешивание данных внутри каждого столбца формы; AddRoundKey — сложение ключа раунда с формой.

Алгоритм шифрования ГОСТ основан в 1989 году в СССР и в результате стал Федеральным стандартом шифрования Российской Федерации. В основе алгоритма лежит сеть Фейстеля. Использует 128 битный ключ шифрования и является надежным. Быстродействие достаточно низкое, но позволяет увеличить скорость работы за счет возможности изменения настроек со снижением криптостойкости.

Алгоритм шифрования RSA (Rivast, Shamir и Adelman, 1977 год) предполагает, что посланное закодированное сообщение может быть прочитано только адресатом. В этом алгоритме используется два ключа — открытый и закрытый. Данный алгоритм привлекателен также в случае, когда большое число субъектов должно общаться по схеме все-со-всеми.

Алгоритм шифрования **El-Gamal** основан в 1985 году Эль-Гамалем. Алгоритм может быть использован для решения всех трех основных задач: для шифрования данных, для формирования цифровой подписи и для согласования общего ключа. Кроме того, возможны модификации алгоритма для схем проверки пароля, доказательства идентичности сообщения и другие варианты. Безопасность этого алгоритма, так же как и алгоритма Диффи-Хеллмана, основана на трудности вычисления дискретных логарифмов. Этот алгоритм фактически использует схему Диффи-Хеллмана, чтобы сформировать общий секретный ключ для абонентов, передающих друг другу сообщение, и затем сообщение шифруется путем умножения его на этот ключ.

В таблице 1 приведены сравнительные оценки показателей (скорость работы, надежность, затрата энергоресурсов ЭВМ) в баллах от 1 до 10 (чем больше балл, тем алгоритм привлекательнее) и известное количество взломов.

Таблица 1

Сравнительная оценка алгоритмов

| Название алгоритма | Скорость | Надежность | Затрата энергоресурсов ЭВМ | Количество взломов |
|---|---|---|---|---|
| Blowfish | 5 | 5 | 4 | 14 |
| DES | 8 | 5 | 2 | 9 |
| CAST | 8 | 6 | 4 | 17 |
| AES | 7 | 7 | 6 | 12 |
| 3DES | 9 | 8 | 6 | 7 |
| RSA | 5 | 5 | 3 | 43 |
| ГОСТ 28147-89 | 5 | 10 | 7 | 0 |
| El-Gamal | 4 | 5 | 4 | 38 |

**Вывод.** Все современные алгоритмы шифрования являются высокоэффективными при использовании ключа не менее 128 бит. Однако в условиях РФ есть смысл использовать алгоритм ГОСТ 28147-89. Он имеет ключ шифрования 256 бит и является достаточно надежным. Для повышения быстродействия алгоритма можно использовать уменьшение длины ключа или уменьшение циклов использования элементов ключа. Однако при таком повышении быстродействия нет сведений об изменении криптостойкости метода. Тем не менее, такой подход часто может быть разумным, например, при необходимости шифрования данных, теряющих свою актуальность в течение нескольких часов. В случае невозможности уменьшения криптостойкости предлагается повысить быстродействие за счет распараллеливания вычислений в мультипроцессорных системах.

**Список использованной литературы:**

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: Триумф, 2003. — 806 с.
2. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. — М.: Аст, Астрель, 2006. — 447 с.
3. http://kriptografea.narod.ru/TDES.html [Электронный ресурс] — дата обращения 12.06.2016 г.

© Шемет В.С., Айдинян А.Р.. 2016

**УДК 658**

**Шишкина Галина Ивановна**
магистрант, ДГТУ
г. Ростов-на-Дону, РФ
E-mail:19galj93@mail.ru
**Суровцева Олеся Анатольевна**
канд. техн. наук, старший преподаватель, ДГТУ
г. Ростов-на-Дону, РФ
E-mail:1354565@mail.ru

## АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ РОССИЙСКИХ ОБУВНЫХ ПРЕДПРИЯТИЙ ЗА 2015 ГОД

**Аннотация**

В статье был произведен анализ производительности обувных предприятий России за 2015 год**.** По результатам проведенного анализа предприятий обувной промышленности был сделан вывод, что наиболее успешной организацией является предприятие ЗАО «ДОНОБУВЬ» так как производительность обуви за 2015 год составляет 900.000 тыс. пар.

**Ключевые слова**

Бенчмаркинг, обувные предприятия, производительность.

В результате выполнения магистерской диссертации был произведен анализ обувных предприятий при помощи бенчмаркетинга.

Бенчмаркинг представляет собой изучение деятельности конкурентов, с целью использования их положительного опыта в своей работе. Также он содержит комплекс средств, которые позволяют систематически находить и оценивать все достоинства опыта других предприятий и внедрять их в свою работу [1, с. 111-113].

В последнее время бенчмаркетинг стал очень популярным. Вследствие, роста конкуренции и в необходимости для компаний в этих условиях выживать, развиваться и достигать прибыли [2, с. 29-30].

В настоящее время обувная промышленность переполнена фирмами, занимающимися производством специальной обуви. По результатам опроса был проведен анализ производительности