Иванов Д.С.
Научный руководитель - к.т.н., доцент каф. ФПМ Штыков Р.А.
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
Ivanov.daniil.666@gmail.com

Обзор и анализ методов шифрование пользовательских данных в ПФР

Необходимость обеспечения безопасности персональных данных в наше время объективная реальность. Информация о человеке всегда имела большую ценность, но сегодня она превратилась в самый дорогой товар. Информация в руках мошенника превращается в орудие преступления, в руках уволенного сотрудника – в средство мщения, в руках инсайдера – товар для продажи конкуренту… Именно поэтому персональные данные нуждаются в самой серьезной защите.

Необходимость принятия мер по защите персональных данных вызвана также возросшими техническими возможностями по копированию и распространению информации. Уровень информационных технологий достиг того предела, когда самозащита информационных прав уже не является эффективным средством против посягательств на частную жизнь. Современный человек уже физически не способен скрыться от всего многообразия явно или неявно применяемых в отношении него технических устройств сбора и технологий обработки данных о людях.

С развитием средств электронной коммерции и доступных средств массовых коммуникаций возросли также и возможности злоупотреблений, связанных с использованием собранной и накопленной информации о человеке. Появились и эффективно используются злоумышленниками средства интеграции и быстрой обработки персональных данных, создающие угрозу правам и законным интересам человека.

Объект исследования в данной работе – шифрование пользовательских данных в ПФР, предмет исследования – шифрование пользовательских данных.

Целью исследования является обзор и анализ методов шифрование пользовательских данных.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Обзор методов шифрования.
2. Анализ типов шифрования.
3. Результаты исследования.

Обзор алгоритмов шифрование пользовательских данных.

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.

Алгоритм шифрования Blowfish основан в 1993 году Брюсом Шнаером. В общем случае алгоритм состоит из двух этапов — расширение ключа и шифрация/дешифрация исходных данных. 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. 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. 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 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.

Анализ типов шифрования.

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. ТВ результате анализа были выявлены следующие достоинства данного метода, приведенные в таблице:

Таблица 1-Результаты анализа

Название алгоритма	Скорость, баллы	Надежность, баллы	Затрата энергоресурсов ЭВМ, баллы	Количество взломов, Шт.
Blowfish	5	5	4	4
DES	8	5	2	9
CAST	8	6	4	17
AET	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

Результаты исследования. В результате проведенного исследования было выяснено, что

выбор типа шифрования напрямую зависит от скорости, надежности, затрат энергоресурса ЭВМ для решения поставленных задач.

Литература

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. Международный научный журнал «символ науки» №6, 2016.