АНАЛИЗ МЕТОДОВ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Рогов М. Г., Шандраков А. Г.

Лещёв А. Е. – ст. преподаватель, магистр техн. наук

В современном мире защита информационных систем от неправомерного вмешательства стала важной, а в некоторых областях и первостепенной задачей. Обеспечение безопасности данных на данном этапе развития информационных технологии приобрело массовый характер. Общение в социальных сетях или рабочая переписка, обмен личными фотографиями или передача коммерческо-важной информации. Несанкционированный доступ сегодня является достаточно серьезной проблемой.

Для предотвращения несанкционированного доступа и увеличения безопасности хранимой информации используются различные методы защиты [2]:

- идентификация (именование и опознавание), подтверждение подлинности (аутентификация) пользователей системы;
- использование разных уровней доступа к ресурсам системы, а также авторизация пользователей (присвоение полномочий);
- обеспечение аудита системы – регистрирование событий и своевременное оповещение о всех событиях, происходящих в системе ;
- шифрование хранимой и передаваемой по каналам связи информации;
- проверка подлинности (целостности, аутентичности и авторства) данных;
- обеспечение защиты системы от действий компьютерных вирусов (выявление и нейтрализация;
- выявление уязвимостей (слабых мест) системы;
- изоляция (защита периметра) компьютерных сетей;
- обнаружение атак и оперативное реагирование, и ряд других методов и механизмов.

Криптографические методы защиты базируются на реализации некоторого преобразования информации. Это преобразование осуществляется пользователям системы (либо несколькими пользователями), если у него в распоряжении имеется некоторый секретом. Без знания секрета (за приемлемое время с практически нулевой вероятностью) невозможно осуществить преобразование информации [3].

К криптографическим методам защиты, при рассмотрении с общей точки зрения, относятся:

- шифрование (дешифрование) информации;
- формирование и проверка цифровой подписи электронных документов.

Существует огромное количество задач по защите информации и данных. Применение криптографических методов позволяет:

- предотвратить возможность ознакомится с данными при их хранении в компьютере или на переносных носителях, а также при передаче по каналам связи без прав доступа;
- подтвердить подлинность электронного документа, доказать авторства документа и факта его получения от соответствующего источника информации;
- обеспечить имитостойкость (гарантию целостности) - исключение возможности необнаружения несанкционированного изменения информации;

В ходе работы был проведен анализ функционирования информационных систем на основе применяемых методов защиты двух наиболее распространенных операционных систем – Windows и Linux. Были выявлены положительные и отрицательные особенности использования различных методов защиты в операционных системах. Исследование позволило выявить наиболее практичные методы защиты как с точки зрения удобства для рядового пользователя, так и со стороны энергозатратности системы.

Список использованных источников:

6. Смарт Н. Cryptography: An Introduction / Н. Смарт – Москва: «Техносфера», 2006. – 528 с.
7. Скембрей Дж. Секреты хакеров / Дж. Скембрей, Ст. Мак-Клар – Москва: «Вильямс», 2004. – 512 с.
8. Манн С. Безопасность Linux / С. Манн, Э. Митчелл, М. Крелл – Москва: «Вильямс», 2003. – 524 с.