

УДК 004.4

## КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ДАННЫХ

*Кочедыкова Е.О., студентка 1 курса факультета ветеринарной  
медицины и биотехнологии  
Научный руководитель – Заживнова О.А., кандидат  
экономических наук, доцент  
ФГБОУ ВО Ульяновский ГАУ*

**Ключевые слова:** Криптография, решаемые задачи, шифрование, ключ, защита.

*Работа посвящена изучению вопроса о криптографии и ее практического значения в жизни людей.*

Термин «криптография» в переводе с древнегреческого означает «секретный шрифт». Эта наука занимается шифрованием текстов и других данных для дальнейшей защиты от нежелательных пользователей. Как доказали ученые, тексты начали шифровать уже в третьем тысячелетии до нашей эры. Как в Римской империи, так и в Средневековье важные сообщения и военные приказы зашифровывались с помощью криптографии.

На сегодняшний день появляются новые информационные технологии, развиваются надежные компьютерные системы хранения, обработки данных, повышаются уровни защиты информации [5]. При этом возросла необходимость повышения эффективности защиты вместе с усовершенствованием хранения данных. Поэтому защита различных персональных данных – неотъемлемая часть жизни любой коммерческой организации, деятельности органов власти. Из-за постоянного роста количества внешних и внутренних угроз возникает необходимость в эффективной защите системы [1].

Также довольно часто применяется криптографическая защита информации – «КАРМА» - технология криптозащиты и электронная подпись для любых приложений. Основная функция продукта «КАРМА» – обеспечение защиты и шифрования персональных данных пользователя [2].

Применяется в любых программных продуктах, где необходимо использование средств криптозащиты. Это системы:

- электронного документооборота, в том числе юридически значимого;

- транспортного назначения (почтовые программы, системы гарантированной доставки сообщений);
- обеспечения принятия управленческих решений, интеграционные среды;
- автоматизации бизнес-процессов;
- кадровые;
- бухгалтерские, в том числе «1С»;
- WEB-приложения, информационные порталы;
- архивные системы, электронные хранилища документов;
- информационно-справочные;
- прикладные, персонального использования.

«КАРМА» может применяться непосредственно пользователем MS Windows для подписания и шифрования файлов в проводнике MS Windows.

Для обычного пользователя она предоставляет визуальный интерфейс с набором команд, а для программиста – СОМ интерфейс с набором высокоуровневых операций работы с электронной подписью и сертификатами. Для обычного пользователя достаточно иметь общие сведения об электронной подписи (ЭП), не зная особенностей криптографии. Чтобы использовать функционал цифровой подписи документов и шифрования программного продукта «КАРМА», достаточно изучить представленный на данном сайте материал.

Это простая в управлении многофункциональная система. Она может работать с ЭП, сертификатами, шифровать, а также расшифровывать данные, добавлять в состав подписи графические изображения. Она позволяет широко использовать весь функционал электронной подписи, существенно расширяя возможности ее применения [3].

Система дает возможность ввода изображения печатей, штампов. Для этого необходимо иметь изображения привычных штампов и печатей на тех же местах, где их принято ставить на бумаге. Визуально на экране компьютера такие электронные копии становятся практически неотличимыми от бумажных (рис 1).

Также «КАРМА» позволяет создавать рукописный «стикер» – подобно наклейке, прикрепляемой к бумажному экземпляру. «Стикер» может содержать краткие комментарии, замечания или поручения. Таким образом, технология работы с электронным документом может быть максимально приближена к привычной работе с бумажным носителем (рис.2).

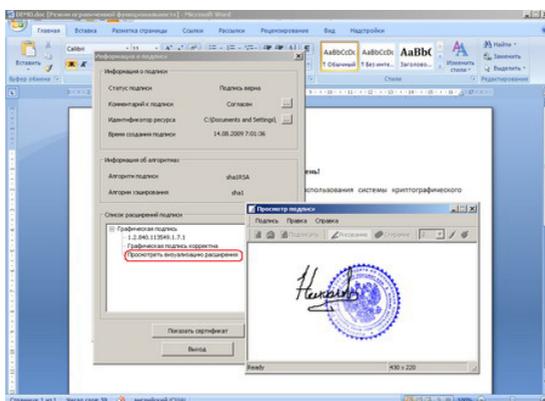


Рисунок 1

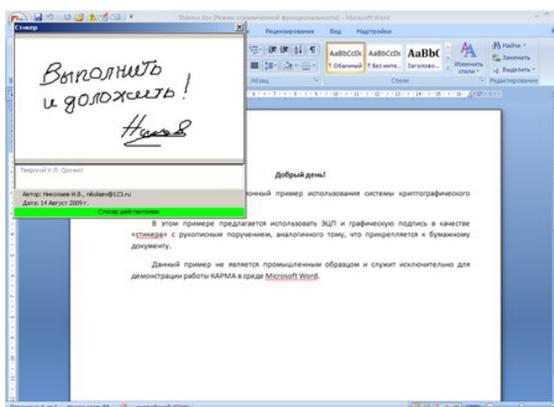


Рисунок 2

Таким образом, можно отметить, что криптографические методы защиты являются удобными в использовании и помогают отлично защитить все персональные данные пользователей [4].

#### Библиографический список:

1. Криптографическая защита персональных данных [Электронный ресурс]: официальный сайт. - Краснодар: ИС, 2019. - Режим доступа: <http://www.rosint.net/content/132>

2. Криптографическая защита информации [Электронный ресурс]: официальный сайт. - М. : ЭОС, 2019. - Режим доступа: [https://www.eos.ru/eos\\_products/eos\\_karma](https://www.eos.ru/eos_products/eos_karma)
3. Что такое криптография? Просто о сложном [Электронный ресурс].- Режим доступа: <https://ichip.ru/chto-takoe-kriptografiya-prosto-o-slozhnom.html>
4. Романов, В.В. Информационные системы и технологии в экономике: Учебное пособие для специальностей экономического профиля / В.В. Романов, О.В. Солнцева, А.В. Севастьянов, О.А. Заживнова – Ульяновск, 2015. – 134 с.
5. Голубев, С.В. Информационная безопасность в автоматизированных системах управления / С.В. Голубев, С.А. Голубева, Е.А. Голубева // Материалы VIII Международной научно-практической конференции молодых ученых «Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения». -Ульяновск: УлГАУ, 2017. – С. 31-34.

## **CRYPTOGRAPHIC DATA PROTECTION METHODS**

***Kochedykova E. O.***

**Key words:** *cryptography, solved problems, encryption, key, protection.*

*The work is devoted to the study of cryptography and its practical importance in people's lives.*