**УДК 004.056.55**

**А.Н. Кокоулин, А.Р. Ахматшин**
Пермский национальный исследовательский
политехнический университет, г. Пермь

# ПЕРСПЕКТИВЫ РАЗВИТИЯ КРИПТПРОВАЙДЕРОВ

Приводится описание криптопровайдеров и их сравнение с другими криптографическими средствами защиты, а также рассмотрены перспективы их развития. Целью статьи является обобщение данных для проведения дальнейшего исследования.

**Ключевые слова:** информационная безопасность, операционные системы, криптопровайдер.

**A.N. Kokoulin, A.R. Akhmatshin**
Perm national research polytechnic university, Perm

# OPPORTUNITIES FOR THE DEVELOPMENT CRYPTO PROVIDERS

This article describes the crypto providers and their compare with other cryptographic security facilities, as well as opportunities for the development. The purpose of the article is to compile data for further research.

**Keywords:** information security, operating systems, crypto provider.

Каждый день в сети Интернет люди обмениваются друг с другом огромным объёмом информации, и многие не подозревают какой путь она преодолевает и как меняет свою форму. В силу экспоненциального увеличения объёма данных в Интернете и незнания точных механизмов её преобразования в сети у людей появилась повышенная потребность в обеспечении информационной безопасности, т.е. в защите своих данных от злоумышленников. Для удовлетворения этой потребности совершенствуются старые или создаются новые механизмы защиты информации, которые внедряются в предметы повседневной жизни людей. Одним из таких механизмов являются криптопровайдеры.

Криптопровайдером (Cryptographic Service Provider – CSP) называется специальная независимая библиотека, способная осуществлять криптографические операции в операционных системах (ОС) под управлением криптографического интерфейса. Использование криптопровайдеров подразумевает как реализацию базовых криптографических алгоритмов, так и существенное расширение списка поддерживаемых криптографических алгоритмов в ОС. В сравнении с иными программными средствами криптографической защиты криптопровайдеры обеспечивают более надёжную защиту, которая определяется требованием использования сертификатов при работе с криптопровайдерами и относительную простоту работы, а в сравнении с другими средствами более низкую цену.

Однако стоит заметить, что из-за относительной простоты использовать криптопровайдеры можно не только для защиты информации, но также для осуществления вредоносных целей путём разработки вирусов. Эта тенденция прослеживалась при создании криптопровайдеров и в то время вирусы реализовывались достаточно примитивно. В настоящее время снова появляются аналогичные вирусы, но с более сложной реализацией. Это поспособствует разработке новых механизмов защиты приложений с использованием криптопровайдеров.

Раньше одним из недостатков использования криптопровайдеров можно было отметить плохую кроссплатформенность, т.е. реализацию на разных ОС и устройствах. Сейчас же криптопровайдеры используются не только для создания программных средств защиты, а также для разработки аппаратных и аппаратно-программных средств защиты.

Отдельно стоит выделить современное использование криптопровайдеров для создания защищённых облачных сервисов, которые набирают популярность, и для улучшения защиты данных пользователей в сети Интернет через дифференциальную конфиденциальность и обезличивание данных.

С начала 2000-ных годов потребность людей в обеспечении информационной безопасности резко возросла, как и интерес к криптопровайдерам. Это прослеживается также в отношении обыкновенных пользователей интернета, что повлекло к созданию готовых решений, удобных в использовании для обыкновенных людей.

## Список литературы


1. Строжевский Юрий (2005-2016), Использование C Software Developer Networks Magazine, No. 5, 2004.

2. Aaron Zimba, Zhaoshun Wang, Hongsong Chen and Mwenge Mulenga (2019), Recent Advances in Cryptovirology: State-of-the-Art Crypto Mining and Crypto Ransomware Attacks. KSII Transctions On Internet And Information Systems vol. 13, no. 6, Jun. 2019.

3. Florian Reimair, Johannes Feichtner, Dominik Ziegler, Sandra Kreuzhuber and Thomas Zefferer (2017), Cryptographic Service Providers in Current Device Landscapes: An Inconvenient Truth. ICETE vol. 4, 2017.

4. Amrita Roy Chowdhury, Chenghong Wang, Xi He, Ashwin Machanavajjhala and Somesh Jha (2019), Crypt: Crypto-Assisted Differential Privacy on Untrusted Severs. 33rd Conference on Neural Information Processing Systems.

5. Adam L. Young (2006), Cryptoviral extorting using Microsoft’s Crypto API. International Journal of Information Security, No. 4, 2006.

**Сведения об авторах**

**Кокоулин Андрей Николаевич** – кандидат технических наук, доцент кафедры «Автоматика и телемеханика», Пермский национальный исследовательский политехнический университет, г. Пермь, email: a.n.kokoulin@gmail.com

**Ахматшин Артём Ринатович** – магистрант Пермского национального исследовательского политехнического университета, гр. КЗИ-19-1м, г. Пермь, email: frexort@mail.ru

**About the authors**

**Kokulin Andrey Nikolaevich** – Candidate of Technical Sciences, Associate Professor of the Department of Automation and Telemechanics, Perm National Research Polytechnic University, Perm, email: a.n.kokoulin@gmail.com

**Akhmatshin Artyom Rinatovich** – Master's student of the Perm National Research Polytechnic University, gr. KZI-19-1m, Perm, email: frexort@mail.ru