A. V. Gorlatyh, P. V. Smirnov

Identity Management Systems Cryptographic Protection Methodology Development

Key words: identity management, cryptography, informational security.

This work proposes methods of identity management systems cryptographic protection. At the moment, there is no cryptographic software, which can be fully used under Russian Federation law circumstances. That' s why, solution that relies on integration of open-source identity management system and certified cryptographic software is proposed.

А. В. Горлатых, П. В. Смирнов

РАЗРАБОТКА МЕТОДОЛОГИИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ СИСТЕМ УПРАВЛЕНИЯ ИДЕНТИФИКАЦИОННЫМИ ДАННЫМИ

В результате своего развития человечество все глубже погружается в мир цифровых технологий. Рост числа электронных сервисов и приложений в информационной инфраструктуре организации приводит к тому, что становится все сложнее управлять идентификационной информацией. Вследствие отсутствия централизованного подхода в данном процессе в системах безопасности появляются уязвимости, связанные с учетными записями пользователей.

Под управлением идентификационной информацией понимается процесс автоматизации процедуры аутентификации пользователей и контроля доступа к ресурсам системы, основанного на правах и ограничениях аутентифицированного субъекта [1].

Согласно «Положению о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» [2] (приказ ФСБ России от 9 февраля 2005 г. № 66) при организации криптографической защиты информации конфиденциального характера в государственных органах и организациях, выполняющих государственные заказы, средства криптографической защиты информации, которые используются для защиты информации конфиденциального характера, должны удовлетворять требованиям по безопасности, устанавливаемым в соответствии с законодательством РФ.

В настоящее время не существует систем управления идентификационными данными, которые полностью соответствовали бы законодательству РФ.

В работе были рассмотрены основные технологии систем управления идентификационными данными, а также принципиальные схемы наиболее популярных протоколов, используемых в системах управления идентификационными данными.

На следующем этапе были проанализированы существующие на данный момент решения, а также обоснован выбор конкретной системы для встраивания в нее сертифицированного СКЗИ.

В ходе работы была проведена модификация криптографического модуля целевых систем, которая позволила использовать в данных продуктах криптографические преобразования, реализованные по

алгоритмам ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94 и ГОСТ 28147-89. Была разработана методика криптографической защиты с применением сертифицированных средств КриптоПро JCP и КриптоПро JTLS. Данная методика была применена и опробована на тестовом стенде.

Предлагаемая методика позволяет использовать комплекс в соответствии с законодательством Российской Федерации в сфере криптографической защиты информации, тем самым расширяя область применения систем управления идентификационными данными.

СПИСОК ЛИТЕРАТУРЫ:

1.Отчет «Сокращение риска несанкционированного доступа к информационным ресурсам кредитной организации с помощью управления доступом к учетным данным» [Электронный ресурс] / Компания Индид. 2012. URL: http://expo-itsecurity.ru/ upload/iblock/4d5/Obzor_risky%20nsd.pdf (дата обращения: 04.04.2014).

2.Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)». Зарег. в Минюсте РФ 3 марта 2005 г., рег. № 6382.

REFERENCES:

1.Otchet “Sokrashchenie riska nesanktsionirovannogo dostupa k informatsionnym resursam kreditnoi organizatsii s pomoshchiu upravleniya dostupom k uchetnym dannym”. 2012. URL: http://expo-itsecurity.ru/upload/iblock/4d5/Obzor_risky%20nsd.pdf.

2.Prikaz FSB RF ot 9 fevralya 2005 g. № 66 “Ob utverzhdenii Polozheniya o razrabotke, proizvodstve, realizatsii i ekspluatatsii shi- frovalnyh (kriptographicheskih) sredstv zashity informatsii (Polozhenie PKZ-2005)”.