УДК 004.056.55

# *СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

***Веретенников К. П.,***

*бакалавр, направление подготовки «Информационная безопасность»,*

*Национальный исследовательский Мордовский государственный университет им. Н.П. Огарева,*

*г. Саранск, Россия*

**Аннотация:** В данной статье исследуется сущность понятия «средства криптографической защиты информации» (СКЗИ) и их основные виды, описывается актуальность СКЗИ в настоящее время, а также дается характеристика направлений их использования.

**Ключевые слова:** средства технической защиты информации, криптографическая защита информации, секретность, информационная безопасность, криптопровайдер, алгоритм.

# *MEANS OF CRYPTOGRAPHIC PROTECTION OF INFORMATION AS A TOOL TO ENSURE INFORMATION SECURITY*

***Veretennikov K. P.***

*Bachelor*

*Ogarev Mordovia State University,*

*Saransk, Russia*

**Abstract:** This article examines the essence of the concept of «means of cryptographic protection of information», their relevance at the present time, and also describes the directions of their use.

**Keywords**: means of technical protection of information, cryptographic protection of information, secrecy, information security, cryptographic provider, algorithm.

Криптографическая защита информации считается одним из самых надёжных способов защиты используемой, обрабатываемой и передаваемой информации, ведь она сохраняет саму информацию, а не доступ к ней. Информация, преобразованная с использованием криптографических методов, обладает повышенной степенью защиты с сохранением необходимого уровня секретности.

Криптографическая защита информации позволяет защитить информацию от её подмены злоумышленником и однозначно установить её правообладателя посредством проверки установленной электронной подписи.

Криптографическая защита информации позволяет закрыть для посторонних лиц информацию конфиденциального характера с применением средств и механизмов шифрования. И даже, используя открытые каналы связи, злоумышленники доступ к информации получить не смогут.

Так что же такое СКЗИ?

СКЗИ – это аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие различные алгоритмы криптографического преобразования информации и предназначенные как для защиты информации при её передаче по каналам связи, так и для защиты информации от несанкционированного доступа при её обработке и хранении [1].

СКЗИ обеспечивают защиту информации по самым важным параметрам, таким как конфиденциальность (отсутствие доступа к информации, если на это нет прав), целостность и аутентификация (отсутствие возможности несанкционированного изменения данных), авторство (подтверждение действий пользователя и невозможность отказа от них).

На сегодняшний день при шифровании используются различные алгоритмы, как симметричные, так и асимметричные. Длина используемых

ключей достаточна для того, чтобы обеспечить необходимую криптографическую сложность и защищённость информации.

Самые популярные алгоритмы, которые используются в криптозащите:

– симметричный ключ – DES, AES, RC4, российский Р-28147.89 и другие;

– с хеш-функциями – например, SHA-1/2, MD4/5/6, Р-34.11.94 и другие;

– асимметричный ключ – RSA и другие.

СКЗИ может быть встроена в физический носитель (аппаратная криптозащита), представлена как отдельный программный продукт (программная криптозащита) или же совмещать аппаратную и программную криптозащиту (аппаратно-программная криптозащита).

Аппаратные СКЗИ – это физические устройства, содержащие специальные программы, обеспечивающие надёжное шифрование данных. С их помощью обеспечивается хранение информации, её запись и передача. Аппаратные СКЗИ устанавливаются довольно быстро и способны с большой скоростью обмениваться информацией, но у них достаточно высокая стоимость и ограниченная возможность для последующей модернизации.

Программные СКЗИ – это комплекс программ, обеспечивающий шифрование информации на различных физических носителях (флэшках, жёстких и оптических дисках и других), а также при её передаче по каналам связи (сети Интернет, электронной почте, локально-вычислительной сети и так далее). Программные СКЗИ в основном используются в тех областях, где нет серьёзных требований к стойкости и функциональности системы.

Аппаратно-программные СКЗИ – это комплекс программ и устройств, в котором собраны все самые лучшие свойства аппаратных и программных СКЗИ, и который на сегодняшний день является самым надёжным и защищённым способом обработки информации.

В том или ином виде СКЗИ в своей работе используют федеральные органы исполнительной власти, исполнительные власти государственной власти Российской Федерации, органы местного самоуправления муниципальных

образований и иные органы и организации. Используемые данными органами и организациями СКЗИ соответствуют, или как минимум должны соответствовать, следующим основным национальным стандартам в области криптографической защиты информации:

– ГОСТ Р 34.10-2001. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (в соответствии с письмом ФСБ России от 07.09.2018 N 149/7/6-363 возможность использования схемы электронной подписи, соответствующей ГОСТ Р 34.10-2001 для формирования электронной подписи, продлевается до 31.12.2019);

– ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

– ГОСТ Р 34.11-2012. «Информационная технология. Криптографическая защита информации. Функция хэширования»;

– ГОСТ Р 34.12-2015. «Информационная технология. Криптографическая защита информации. Блочные шифры»;

– ГОСТ Р 34.13-2015. «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров».

Рассмотрим несколько популярных используемых в настоящее время СКЗИ с кратким описанием их функциональных особенностей.

«Криптопровайдер КриптоПро CSP» (производитель ООО «КРИПТО-ПРО») – предназначен для авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством:

– использования процедур формирования и проверки электронной подписи в соответствии с национальными стандартами;

– обеспечения конфиденциальности и контроля целостности информации посредством её шифрования и имитозащиты;

– обеспечения аутентичности, конфиденциальности и имитозащиты соединений по протоколу защиты транспортного уровня (TLS);

– контроля целостности и неизменности системного и прикладного программного обеспечения;

– управления ключевыми элементами системы в соответствии с регламентом средств защиты [2].

ViPNet CUSTOM (производитель ОАО «Инфотекс») – линейка программных и программно-аппаратных комплексов, включающая средства защиты информации ограниченного доступа, в том числе персональных данных, позволяющая организовать защиту информации в организациях и нацеленная на решение двух важных задач информационной безопасности:

– создание защищённой, доверенной среды передачи информации путём организации виртуальной частной сети (VPN);

– развёртывание инфраструктуры открытых ключей (PKI) с целью использования механизмов электронной подписи в системах документооборота и делопроизводства, электронной почте, банковском программном обеспечении, электронных торговых площадках и витринах, с поддержкой возможности взаимодействия с PKI-продуктами других отечественных производителей.

Криптопровайдер ViPNet CSP 4 (производитель ОАО «Инфотекс») – это СКЗИ, предназначенное для выполнения криптографических операций, доступ к которым обеспечивается встраиванием API-криптопровайдера в прикладное программное обеспечение через стандартизованные интерфейсы. Криптопровайдер обеспечивает реализация криптографических алгоритмов, на соответствие национальным стандартам [3].

ViPNet CSP 4 обеспечивает выполнение следующих функций в зависимости от используемой версии операционной системы:

– формирование ключей электронной подписи, ключей проверки электронной подписи, а также ключей шифрования;

– формирование хеш-функции в соответствии с криптографическими алгоритмами;

– формирование и проверка электронной подписи в соответствии с криптографическими алгоритмами;

– формирование случайных и псевдослучайных чисел, а также сессионных ключей шифрования;

– формирование ключей шифрования, так и последующее шифрование и имитозащита данных с использованием сформированных ключей шифрования;

– аутентификация, передача данных по транспортному протоколу передачи данных (TLS);

– операции с сертификатами открытых ключей в соответствии с стандартом ITU-T для инфраструктуры открытого ключа (X.509 v3);

– формирование сообщений формата PKCS #7 (в соответствии с стандартом CMS);

– формирование транспортных ключевых контейнеров в формате PKCS #12 (в соответствии с стандартом PFX).

ViPNet SafeDisk (производитель ОАО «Инфотекс») – программный продукт, предназначенный для организации безопасного хранения конфиденциальной информации и удобной работы с ней на технических средствах, обеспечивая высокий уровень защиты любой информации и может использоваться в государственных структурах и организациях, как СКЗИ, так и средство защиты от несанкционированного доступа.

ViPNet SafeDisk обеспечивает выполнение следующих функций:

– прозрачное шифрование данных, производимое в реальном времени, позволяя работать с документами в обычном режиме.

– информация хранится на жёстком диске или внешнем носителе в контейнере в виде зашифрованного файла и защищается файл-ключом или электронным ключом;

– при подключении внешнего носителя контейнер отображается в системе как обычный логический диск. При отключении внешнего носителя логический диск перестаёт отображаться в системе, поэтому установить факт наличия конфиденциальной информации и получить к ней доступ посторонним лицам не представляется возможным;

– в программе существуют режимы экстренного отключения контейнеров и выхода из программы (режим «Опасность»), а также режим экстренного уничтожения доступа к информации для всех пользователей программы (режим «Большая опасность»).

«КриптоАРМ» (производитель ООО «Цифровые технологии») – программный комплекс для шифрования и электронной подписи файлов, передаваемых как по сети Интернет и электронной почте, так и на съёмных машинных носителях информации (жёстком диске, флэш-карте и другие) [4].

Используется в тех информационных системах, где нужно:

– надёжно защитить конфиденциальные данные (в том числе персональные) от постороннего доступа;

– гарантировать целостность и неизменность данных при отправке по незащищённым каналам связи;

– обеспечить подлинность и авторство обрабатываемых и передаваемых данных;

– использовать электронное согласование документов.

«Континент» (производитель ООО «Код Безопасности») – комплекс программно-аппаратных продуктов для обеспечения сетевой безопасности при подключении к сетям общего пользования (в том числе сети Интернет) посредством межсетевого экранирования, посредством построения частных виртуальных сетей (VPN) и системы обнаружения вторжений (СОВ).

Надёжные высокопроизводительные платформы, высокая криптостойкость шифрования каналов связи, поддержка защиты самых современных коммуникационных приложений в сочетании с простотой

внедрения и эксплуатации гарантируют качественное решение с помощью продуктов семейства «Континент» самых сложных задач защиты корпоративных сетей.

Основные возможности программного-аппаратного комплекса «Континент»:

– надёжная криптозащита, с шифрование трафика с современной ключевой схемой для обеспечения гарантированной криптостойкость VPN-сети;
– межсетевое экранирование;
– маршрутизация трафика;
– управление трафиком;
– интеграция с системами обнаружения вторжения (IDS).

Таким образом, можно сделать вывод о значительном количестве средств криптографической защиты информации. Все они должны обеспечивать достижение следующих целей [6]:

1. Конфиденциальность

Когда необходимо предотвратить разглашение информации посторонним лицам, необходимо соблюдать конфиденциальность. Криптография используется для шифрования информации, чтобы сделать ее непонятной для всех, кроме тех, кто имеет право просматривать ее. Чтобы обеспечить конфиденциальность, криптографический алгоритм и режим работы должны быть спроектированы и реализованы таким образом, чтобы неавторизованная сторона не могла определить ключи, которые были связаны с шифрованием, или иметь возможность получать информацию без использования правильные ключи.

2. Целостность данных

Целостность данных обеспечивает гарантию того, что данные не были изменены несанкционированным образом после того, как они были созданы, переданы или сохранены. Это означает, что не было вставки, удаления или замены данных. Цифровые подписи или коды аутентификации сообщений

являются криптографическими механизмами, которые могут использоваться для обнаружения как случайных изменений, которые могут произойти из-за сбоя оборудования или проблем передачи, так и преднамеренных изменений, которые могут быть выполнены злоумышленником. Хотя некриптографические механизмы могут быть использованы для обнаружения случайных изменений, они не являются надежными для выявления преднамеренных изменений.

3. Аутентификация

Криптография может предоставлять два типа услуг аутентификации:

Аутентификация целостности может использоваться для проверки того, что данные не подвергались модификации.

Аутентификация источника может использоваться для проверки личности того, кто создал информацию, например, пользователя или системы.

Цифровые подписи или коды аутентификации сообщений чаще всего используются для предоставления услуг аутентификации. Методы согласования ключей также могут быть использованы для предоставления этой услуги.

4. Авторизация

Авторизация предоставляет разрешение на выполнение функции безопасности или действия. Эта служба безопасности часто поддерживается криптографической службой. Авторизация обычно предоставляется после успешного выполнения службы аутентификации источника.

5. Неотрекаемость

В управлении ключами термин «отказ от авторства» относится к связыванию субъекта сертификата посредством использования ключей цифровой подписи и цифровых сертификатов с открытым ключом. Когда для ключа цифровой подписи требуется отказ от авторства, это означает, что подпись, созданная этим ключом, поддерживает как службы целостности, так и службы аутентификации источника цифровой подписи. Цифровая подпись может также указывать обязательство субъекта сертификата таким же образом, как документ с рукописной подписью.

6. Службы поддержки

Вспомогательные сервисы часто требуются для вышеуказанных базовых криптографических сервисов безопасности. В качестве примера, криптографическому сервису часто требуются сервисы для установления ключей и генерации случайных чисел, а также защиты самих криптографических ключей.

7. Объединение услуг

Настоятельно рекомендуется объединить вышеперечисленные шесть служб безопасности. При разработке защищенной системы проектировщики обычно начинают с определения того, какие системы безопасности необходимы для защиты информации, которая будет храниться и обрабатываться системой. Как только услуги определены, рассматриваются механизмы, которые будут наилучшим образом предоставлять эти услуги.

Некоторые из выбранных механизмов могут не иметь криптографического характера. Например, меры физической безопасности, такие как идентификационные значки или устройства биометрической идентификации, могут использоваться для ограничения доступа к определенным данным в целях конфиденциальности. Тем не менее, криптографические механизмы, которые включают в себя алгоритмы, ключи или другие ключевые материалы, как правило, являются наиболее экономически эффективными методами для обеспечения безопасности информации.

8. Управление ключами

Правильное управление криптографическими ключами имеет важное значение для уровня безопасности, который может быть достигнут в системе с помощью криптографии. Эта достижимая безопасность зависит от различных факторов, таких как архитектура криптографической системы или применяемое сочетание механизмов и их внутренняя устойчивость к атакам.

Таким образом, в настоящее время СКЗИ используются во многих сферах жизнедеятельности человека, таких как электронная отчётность при

представлении её в контролирующие органы, электронные торги на федеральных и коммерческих электронных площадках, счета-фактуры в электронном виде, обмен документами, заверенными электронной подписью при взаимодействии различных организаций, арбитражный процесс при банкротстве организаций и продаже имущества про помощи арбитражных управляющих и многие другие. Данный перечень, как мне думается, не окончательный и будет со временем только расширяться, в том числе и за счёт расширения линейки предлагаемых производителями аппаратных, программных и программно-аппаратных СКЗИ.

**Библиографический список:**

1. Немчинова А. С. Кибератаки: понятие, цели и последствия / А. С. Немчинова, К. А. Семерной // Экономика и социум. – 2018. – № 4(47). – С. 920-924
2. Официальный сайт компании КриптоПро [Электронный ресурс]. – Режим доступа: https://www.cryptopro.ru/products/csp
3. Официальный сайт Группы компаний Инфотекс [Электронный ресурс]. – Режим доступа: https://infotecs.ru
4. Официальный сайт ООО «Цифровые технологии» [Электронный ресурс]. – Режим доступа: https://www.trusted.ru
5. Turner M. Applying Cryptographic Security Services – a NIST summary / M. Turner // https://www.cryptomathic.com/news-events/blog/applying-cryptographic-security-services-a-nist-summary

*Оригинальность 82%*