Электронная подпись в системе МВД России

Султанов
Рустам Айратович,
начальник отделения криптографической защиты информации и электронной подписи центра информационных технологий, связи и защиты информации МВД по Республике Башкортостан, майор внутренней службы

Бурное развитие IT-технологий и глобальное распространение локальных и мобильных информационных сетей обеспечило в современном мире масштабный рост обмена электронными документами между различными участниками электронно-информационного взаимодействия.

Электронный оборот документов между пользователями информационных сетей содержит различную информацию, которая по своим признакам и характеристикам имеет свою ценность — государственную, коммерческую или частную и обладает конфиденциальным статусом. Несомненно, такая информация, проходящая массивными потоками через открытые и доступные информационные сети, вызывает немалый интерес у различных заинтересованных лиц, не имеющих к ней права доступа, т. е. разрешение обладателя информации[1]. В данной ситуации возникает проблема безопасности информации[2] и ее защита от несанкционированного доступа с использованием различных злоумышленных действий, к которым относятся: (рис. 1)

- перехват — злоумышленник, подключается к сети, перехватывает документы (файлы) и вносит в них изменения;
- маскарад (самозванство) — злоумышленник направляет документ пользователю В от имени пользователя А;
- отказ (ренегатство) — пользователь А заявляет, что не направлял сообщение пользователю В, хотя на самом деле направил;
- подмена — пользователь В изменяет или формирует новый документ и заявляет, что получил его от пользователя А;
- повтор — злоумышленник повторяет ранее переданный документ, который пользователь А направил пользователю В.

Такие виды злоумышленных действий наносят существенный ущерб банковским и коммерческим структурам, государственным предприятиям и организациям, а также частным лицам, применяющим в своей деятельности информационные технологии[3].

Таким образом, остро встаёт проблема аутентификации[4] автора документа и самого документа (аутентификация информации[5]), т. е. установления подлинности автора и отсутствия изменений в полученном документе. Обычно в бумажном документе информация и рукописная подпись автора жестко связана с физическим носителем (бумагой). В электронных документах на машинных носителях такой связи нет. При обработке документов в электронной форме совершенно непригодны традиционные способы установления подлинности по рукописной подписи и оттиску печати на бумажном документе. Принципиально новым решением является электронная подпись.

Электронная подпись

Электронная подпись представляет собой комбинацию символов, которая формируется в результате математического преобразования исходного документа при помощи специального программного обеспечения. ЭП добавляется к исходному документу при пересылке, и любое изменение исходного документа делает эту ЭП недействительной. ЭП является уникальной для каждого документа и невозможность подделки ЭП обеспечивается беспредельно высоким количеством математических вычислений, необходимых для её подбора.

Таким образом, ЭП безошибочно указывает на подлинность и авторство, не переносится с одного документа на другой документ, защищает подписанный документ от подделки, а также от изменения или искажения информации (целостность) и несет принцип неотрекаемость, что предотвращает отказ от авторства. ЭП позволяет убедиться в том, что после подписи документа конкретным человеком никто «незаметно» этот документ не изменит, проверит надежность отправителя электронного документа и сохранность его содержания, однозначно определит автора электронного документа и укажет дату подписания.

Электронная подпись основана на асимметричном криптографическом алгоритме. Особенностью такого алгоритма является то, что используются два разных ключа: один ключ для зашифрования информации, а вто-

1 Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

2 Безопасность информации (информационная безопасность) — состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

3 Информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

4 Аутентификация — проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

5 Аутентификация информации — установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации, установление законным получателем (возможно арбитром) факта, что полученная информация наиболее вероятно была передана законным отправителем (источником) и что она при этом не заменена и не искажена.

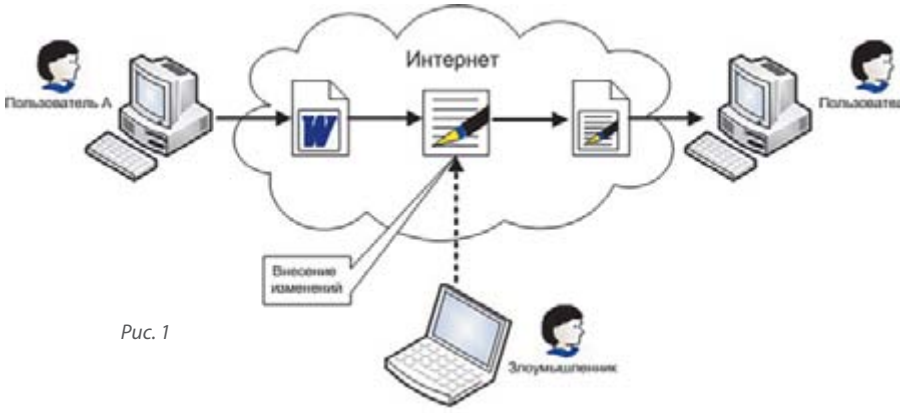

Рис. 1

рой — для ее расшифрования, который специальным образом получен из первого и отличен от него. В симметричном криптоалгоритме для зашифрования и расшифрования используется один и тот же ключ, который известен отправителю и получателю информации и хранится ими в секрете, поэтому симметричные ключи называют секретными.

В асимметричном криптоалгоритме первый ключ является секретным — закрытым (личным) ключом[6], он известен только лицу, подписывающему документ. Второй ключ несекретный — открытый ключ[7], он может быть известен любому получателю электронного документа. Оба этих ключа создаются с помощью специальной криптографической программы (например, «КриптоПро CSP»). Сначала создается закрытый ключ, затем на основании закрытого ключа создается открытый ключ. Обратный процесс — подобрать закрытый ключ по открытому ключу — невозможен. Открытый ключ публикуется на сайте **удостоверяющего центра**, услугами которого пользуется владелец ключа, а закрытый ключ он хранит со всеми возможными мерами предосторожности.

В области применения ЭП удостоверяющий центр выполняет такую же роль, как нотариус в жизненном цикле взаимодействия юридических или физических лиц, для которых необходимо убедиться в подлинности документа, подписанного владельцем. Нотариус проверяет его дееспособность и удостоверяет собственноручную подпись владельца на документе. Таким образом, подпись лица удостоверенная нотариусом, безоговорочно принимается третьими лицами, а в информационном взаимодействии удостоверяющему центру доверяют все участники обмена электронными документами.

Рис. 2

- Удостоверяющий центр (УЦ) является системой управления ключами в рамках криптографической системы[8] на основе инфраструктуры открытых ключей (англ. PKI –закрытый ключ известен только его владельцу);
- удостоверяющий центр создает сертификат открытого ключа и таким образом удостоверяет этот ключ;
- никто не доверяет друг другу, но все доверяют удостоверяющему центру;
- удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа лицу, которое владеет соответствующим закрытым ключом.

Фактически, PKI представляет собой криптографическую систему, основным компонентом которой является УЦ и пользователи, взаимодействующие между собой посредством удостоверяющего центра.

Удостоверяющий центр или Центр сертификации — это организация, которая выпускает сертификаты ключей проверки ЭП и отвечает за управление криптографическими ключами пользователей. Открытые ключи и другая информация о пользователях хранится удостоверяющими центрами в виде цифровых сертификатов.

Сертификат — это цифровой документ, который содержит открытый ключ пользователя УЦ и подписан ЭП уполномоченного лица УЦ[9]. Выдавая сертификат УЦ удостоверяет подлинность связи между открытым ключом пользователя УЦ и информацией, его идентифицирующей.

И ключ (рис. 3), и сертификат хранятся в файлах. Для того, чтобы никто, кроме владельца подписи, не мог воспользоваться закрытым ключом, его обычно записывают на съемный носитель ключа (например «Рутокен»). Его так же как банковскую карточку для дополнительной защиты снабжают PIN-кодом. И точно так же, как при операциях с картой, перед тем, как

6 Закрытый ключ электронной подписи — уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной подписи с использованием средств электронной подписи.

7 Открытый ключ электронной подписи — уникальная последовательность символов, соответствующая закрытому ключу электронной подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной подписи подлинности электронной подписи в электронном документе.

8 Криптографическая система (криптосистема) — система обеспечения безопасности защищённой сети, использующая криптографические средства.

9 Уполномоченное лицо УЦ — осуществляет заверение от лица УЦ сертификатов ключа проверки ЭП, копий сертификатов ключа проверки ЭП и списков отозванных сертификатов ключа проверки ЭП, принимает решения по заявлениям пользователей УЦ о регистрации, изготовлении и аннулировании (отзыве), приостановлении/возобновлении действия сертификата ключа проверки ЭП.

Рис. 3

воспользоваться ключом для создания электронной подписи, надо ввести правильное значение PIN-кода.

Сертификат содержит всю необходимую информацию для проверки электронной подписи. Данные сертификата открыты и публичны. Поэтому обычно сертификаты хранятся в хранилище сертификатов операционной системы (в каждом компьютере, в общем сетевом хранилище, в базе данных и т. п.). И конечно, все сертификаты всегда хранятся в Удостоверяющем центре.

Как работает электронная подпись.

Когда пользователь (отправитель) подписывает электронный документ, происходит следующее: (рис. 4)

1. Программа преобразует исходный текст документа в некий набор символов (контрольная сумма — хэш-функция), который точно соответствует тексту документа. Если документ будет изменен, то контрольная сумма тоже изменится.
2. Затем полученная контрольная сумма шифруются закрытым ключом отправителя.
3. Вместе с электронным документом отправляются контрольная сумма и открытый ключ отправителя.
4. Когда электронный документ получен, программа получателя берет открытый ключ отправителя, присланный с письмом, и с его помощью расшифровывает полученную контрольную сумму.
5. Затем программа генерирует контрольную сумму для текста письма и сверяет обе контрольные суммы. Если присланная контрольная сумма и вторично полученная программой контрольная сумма совпадают, значит — письмо не изменялось.

Таким образом, процедура проверки подлинности ЭП при обработке документов определяет целостность электронного документа и авторизацию владельца сертификата. Т. е., ЭП подлинна (проверка подписи по ГОСТ Р 34.10–2001 прошла успешно), владелец сертификата имел право подписывать документ (сертификат вступил в силу, не просрочен, не отозван, содержит необходимые идентификаторы).

СУЦ ОВД РФ

Приказом МВД России от 28.05.2013 года № 294 введена в эксплуатацию Система удостоверяющих центров органов внутренних дел Российской Федерации (СУЦ ОВД).

СУЦ ОВД — автоматизированная система, предназначенная для реализации возможностей средств электронной подписи в подразделениях системы МВД России. Информация, обрабатываемая СУЦ ОВД, является информацией ограниченного доступа, не содержащей сведений, составляющих государственную тайну. Целью СУЦ ОВД является предоставле-

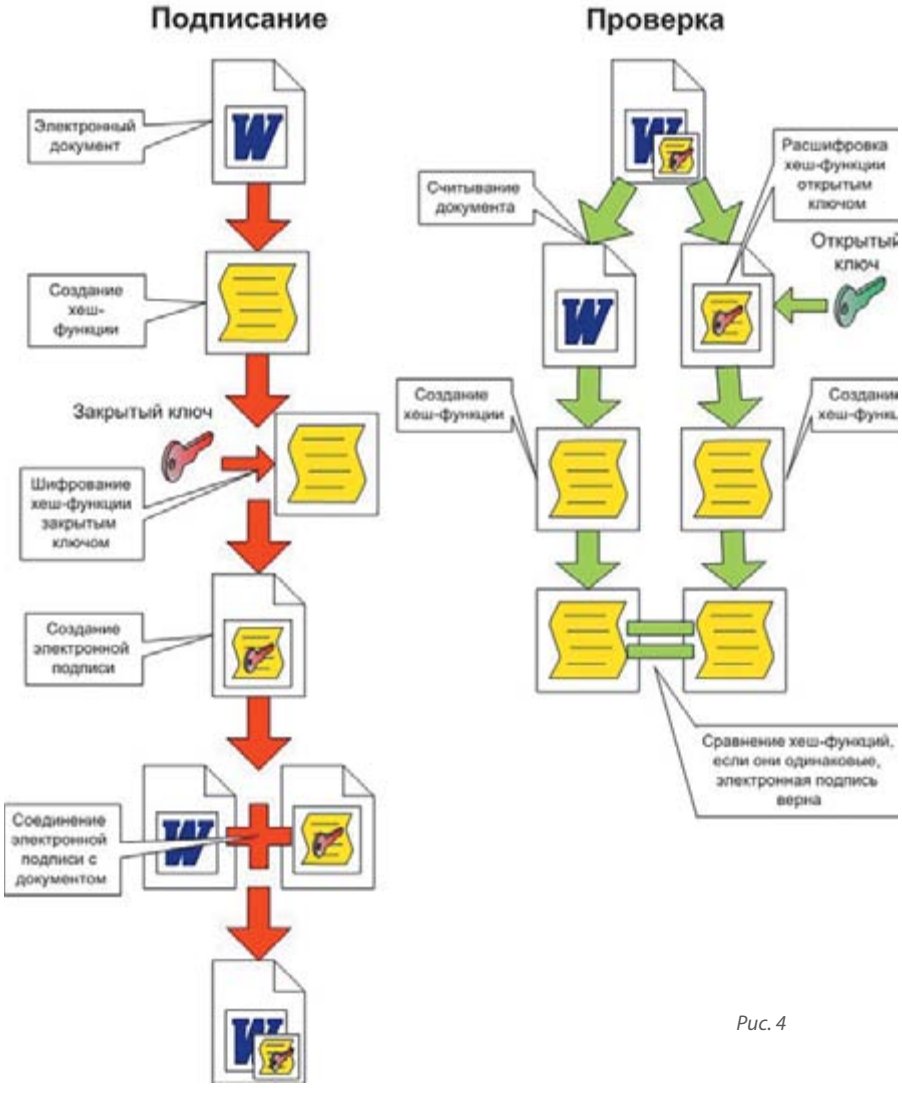

Рис. 4

ние ее пользователям возможностей использования ЭП.

Основными задачами СУЦ ОВД являются:

1. Обеспечение сотрудников ОВД средствами ЭП, в том числе квалифицированными сертификатами ключей проверки электронной подписи (сертификат)[10].
2. Обеспечение проверки ЭП электронного документа и статуса (действительности) сертификатов ключей проверки ЭП пользователей (http://10.0.80.16/svs/).
3. Реализация в СУЦ ОВД методов по обеспечению функционирования средств защиты информации от несанкционированного доступа с целью осуществления сохранности конфиденциальной информации, обрабатываемой в СУЦ ОВД.
4. Обеспечение возможности реализации механизмов строгой аутентификации при доступе пользователей к информационным ресурсам.
5. Обеспечение возможности формирования ЭП электронного документа в целях подтверждения его целостности и авторства и обеспечения юридической значимости.
6. Выполнение процедур по разрешению конфликтных ситуаций, возникающих при использовании средств ЭП.

СУЦ составляет основу инфраструктуры открытых ключей (PKI) в ОВД. В рамках СУЦ обеспечивается контроль выполнения всех процедур, связанных с ключами и цифровыми сертификатами открытых ключей. Целью применения сервисов инфраструктуры открытых ключей является обеспечение реализации механизмов следующих основных функций информационной безопасности:

1. Идентификации и аутентификации субъектов и объектов доступа, а также контроля целостности идентификационных данных.
2. Конфиденциальности передаваемых электронных почтовых сообщений и электронных документов.
3. Целостности электронных документов и подтверждения их авторства.
4. Поддержки механизма разграничения доступа пользователей к информационным ресурсам МВД России.

Функции Удостоверяющего центра МВД России возложены на подразделение, входящее в состав федерального казенного учреждения «Главный центр связи и защиты информации Министерства внутренних дел Российской Федерации», зарегистрированного на территории Российской Федерации в городе Москве.

Удостоверяющий центр осуществляет свою деятельность по созданию и управлению квалифицированными сертификатами ключей проверки ЭП сотрудниками МВД России на территории Российской Федерации на основании Свидетельства об аккредитации удостоверяющего центра от 29 июня 2012 г. №06, выданного Минкомсвязи России.

СУЦ ОВД взаимодействует с единой системой информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России), которая введена в эксплуатацию в апреле 2015 года.

Идентификация в ИСОД МВД России

Одними из основных целей создания и развития ИСОД МВД России это автоматизация основных видов деятельности подразделений МВД России, использование в качестве единого источника информации всеми подразделениями МВД России, организация электронного взаимодействия между ними, обеспечение разграниченного доступа к информационным ресурсам.

В ИСОД МВД России реализована единая политика информационной безопасности, которая обеспечивает санкционированный доступ сотрудников ОВД к информационным системам и ресурсам с автоматизированных рабочих мест и осуществляет контроль и анализ произведенных ими действий.

Для обеспечения санкционированного доступа к сервисам ИСОД на сотрудника заводится учетная запись пользователя для авторизации в системе по логину и паролю. Создание, изменение и блокирование учетной записи пользователей осуществляется при помощи сервиса управления доступом к информационным системам и ресурсам ИСОД МВД России (СУДИС). СУДИС является одним из ключевых элементов подсистемы информационной безопасности ИСОД МВД России (ПОИБ).

Основным механизмом доступа к сервисам ИСОД МВД России (кроме сервиса электронной почты) является реализация процедуры авторизации пользователя с использованием ЭП. Использование процедуры авторизации пользователя по логину и паролю допускается при первичной регистрации в системе и временном отсутствии возможности получения сотрудником ЭП.

После получения учётной записи и «Рутокена» с сертификатом проверки электронной подписи сотруднику необходимо пройти процедуру идентификации и аутентификации на портале СУДИС (http://it.mvd.ru/поиб) и привязать полученный сертификат ЭП к своей учетной записи путем загрузки его в хранилище СУДИС.

В дальнейшем станет возможным осуществлять вход в систему и на сервисы ИСОД МВД России без дополнительного ввода логина и пароля. Производить блокировку АРМ, в случае необходимости временно покинуть рабочее место путем извлечения идентификатора «Рутокен».

Таким образом, использование «Рутокен» с записанным на него сертификатом проверки ЭП обеспечивает санкционированный доступ сотрудника ОВД к сервисам ИСОД МВД России, идентифицирует его в сети информационной системы МВД России от Владивостока до Калининграда. По сути это является электронным аналогом служебного удостоверения сотрудника ОВД.

10 Квалифицированный сертификат ключа проверки электронной подписи — сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром МВД России.