Призначення та сутність стандарту ДСТУ ISO/IEC 9594-8 та який порядок його застосування?

Настоящий стандарт разработан с целью обеспечения взаимосвязи систем обработки информации, предназначенных для предоставления услуг справочника. Совокупность подобных систем вместе с содержащейся в них информацией справочника может рассматриваться как единое целое, называемое справочником. Информация, хранимая справочником и называемая в целом «информационной базой справочника» (ИБС), используется обычно для обеспечения обмена данными между такими объектами, как логические объекты прикладного уровня, персонал, терминалы и дистрибутивные списки.

Справочник играет существенную роль во взаимосвязи открытых систем (ВОС), цель которой состоит в том, чтобы при минимуме технических согласований вне стандартов по ВОС обеспечить взаимосвязь систем обработки информации:

- поставляемых от различных изготовителей;
- использующих различные методы административного управления;
- имеющих различные уровни сложности;
- использующих различные технологии.

Для многих применений требуются средства защиты от угроз нарушения обмена информацией. Некоторые наиболее известные угрозы вместе с услугами защиты и механизмами, которые могут быть использованы для защиты от них, кратко изложены в приложении В. Фактически все услуги защиты зависят от идентичности взаимодействующих сторон хорошо друг другу известных, то есть от их аутентичности.

Настоящий стандарт определяет основы услуг аутентификации, предоставляемых справочником своим пользователям. К этим пользователям относится сам справочник, а также другие прикладные программы и услуги. Справочник может оказаться полезным при обеспечении других потребностей в аутентификации и других услуг защиты, поскольку он представляет собой естественное место, из которого взаимодействующие стороны могут получить информацию друг о друге, то есть сведения, являющиеся основой аутентификации. Справочник — это естественное место потому, что он хранит и другую информацию, необходимую для обмена и полученную до его осуществления. При таком подходе получение из справочника информации аутентификации потенциального партнера подобно получению адреса. Предполагается, что вследствие широкой доступности справочника для целей обмена эти основы аутентификации будут широко использованы многими прикладными программами.

1 **Область применения**

Настоящий стандарт:

- определяет формат информации аутентификации, хранимой справочником;
- описывает способ получения из справочника информации аутентификации;
- устанавливает предпосылки о способах формирования и размещения в справочнике информации аутентификации;
- определяет три способа, с помощью которых прикладные программы могут использовать такую информацию аутентификации для выполнения аутентификации, и описывает, каким образом с помощью аутентификации могут быть обеспечены другие услуги защиты.

В настоящем стандарте изложены два вида аутентификации: простая, использующая пароль как проверку заявленной идентичности, и строгая, использующая удостоверения личности, созданные с использованием криптографических методов. Если простая аутентификация предлагает некоторые ограниченные возможности защиты от несанкционированного доступа, то в качестве основы услуг, обеспечивающих защиту, должна использоваться только строгая аутентификация. Здесь не ставится задача установить эти методы в качестве общей основы аутентификации, но они могут получить общее применение со стороны тех прикладных программ, которые рассматривают эти методы адекватными.

Аутентификация (и другие услуги защиты) могут быть предложены только в контексте определенной стратегии защиты. Пользователи прикладной программы должны сами определить свою собственную стратегию защиты, которая может быть ограничена услугами, предусмотренными стандартом.

Задача стандартов, определяющих прикладные программы, которые используют основы аутентификации, состоит в том, чтобы установить правила протокольных обменов, которые необходимо осуществить для обеспечения аутентификации, основываясь на информации аутентификации, полученной из справочника. Протоколом, используемым прикладными программами для получения удостоверения личности из справочника, является протокол доступа к справочнику (ПДС), определенный в ИСО/МЭК 9594-5.

Метод строгой аутентификации, определенный в настоящем стандарте, основан на криптосистемах ключа общего пользования. Главное преимущество таких систем состоит в том, что сертификаты пользователей могут храниться в справочнике в виде атрибутов, свободно участвовать в обмене внутри системы справочника и могут быть получены пользователями справочника таким же способом, как и любая другая информация справочника. Предполагается, что сертификаты пользователей должны формироваться «автономными» средствами и вводиться в справочник их создателями. Выработка сертификатов пользователей выполняется некоторыми автономными уполномоченными по сертификации (УС), которые полностью отделены от агентов системы в справочнике. В частности, поставщикам справочника не предъявляется никаких специальных требований по записи или обмену сертификатами пользователей надежным способом.