КОМБИНИРОВАННЫЕ МЕТОДЫ ЗАЩИТЫ И КОНТРОЛЯ ДОКУМЕНТАЛЬНЫХ ДАННЫХ

В.К. ЕРОХОВЕЦ, В.Ю. ЛИПЕНЬ, Д.В. ЛИПЕНЬ

Утвержденная 27.12.2002 г. Государственная программа "Электронная Беларусь" предусматривает в своем составе ряд проектов, направленных на создание ведомственных и территориальных автоматизированных информационных систем (АИС), решающих задачу компьютеризации органов госуправления. Одной из таких задач является радикальное расширение сферы использования электронных документов, а также внедрение компьютерного контроля за оборотом выдаваемых гражданам и юридическим лицам бумажных документов (свидетельств ЗАГС, лицензий, справок о собственности) и пластиковых карт (водительских и служебных удостоверений, удостоверений личности и юридических лиц).

Основным отличием внедряемых документов от традиционных является компьютерный способ их изготовления на основе цифровых данных, хранимых в регистрах населения и юридических лиц, а также — в базах данных ведомственных АИС. Такие машинозаполняемые документы могут содержать как традиционные человекочитаемые изображения (текст, фотопортрет, графическое оформление), так и специальные машиносчитываемые маркеры, например, штрих-коды (ШК). Для подобных документов с машиносчитываемой маркировкой могут применяться комбинированные методы защиты и контроля данных. Последние могут включать как процедуры сличения с электронным оригиналом при обращении к базе данных организации-эмитента, так и процедуры автономной верификации, построенные с использованием криптопрограмм, реализующих дешифрирование специальных ШК. Докладчиком демонстрируются примеры бумажных и пластиковых документов с машиносчитываемой маркировкой.

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ДАННЫХ В СИСТЕМАХ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ДЕЙСТВИЯМ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

Е.В. НОВИКОВ

В рамках реализуемой Министерством по чрезвычайным ситуациям Республики Беларусь государственной научно-технической политики в области предупреждения и ликвидации чрезвычайных ситуаций разработана многоуровневая автоматизированная система управления действиями дежурного персонала в чрезвычайных ситуациях, связанных с авариями на химически опасных предприятиях.

Функционирование этой системы, являющейся многоуровневой сетью комплексов, обеспечивающей мониторинг состояния отдельных объектов и передачу данных в соответствующие территориальные подразделения МЧС, невозможно без наличия, кроме прочих компонент, развитых телекоммуникационных средств. В этой коммуникационной среде на каждом уровне генерируется своя информация, объем, и значимость которой возрастают при переходе от одной ступени мониторинга к другой, и вместе с тем растет риск внешних вторжений в деятельность предприятий и органов управления.

Для ликвидации возможных угроз концепция безопасности системы строится с учетом реализации следующих требований:

- обеспечение защиты информации на всех этапах её накопления, обработки и передачи по каналам связи;
- обеспечение защиты информации в каналах связи путем максимального сокращения объемов передачи (передача метаданных, а не полного объема информации) с применением криптографических методов;
- обеспечение целостности и подлинности информации на всех этапах ее хранения, обработки и передачи по каналам связи:
- обеспечение аутентификации сторон, обменивающихся информацией;
- обеспечение контроля доступа к информационным системам и базам данных; а также защита программных продуктов от внедрения программных "вирусов" и закладок.

Разграничение доступа обеспечивается путем использования возможностей операционной системы сервера и средств многопользовательских операционных систем. На всех уровнях разграничения доступа запрещаются все действия, кроме явно разрешенных.

ФОРМИРОВАНИЕ И ИСПОЛЬЗОВАНИЕ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ К ОБЪЕКТАМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

А.А. ГУЛЬКО, Т.С. МАРТИНОВИЧ

В докладе рассматриваются вопросы формирования пакетов функциональных и гарантийных требований безопасности на базе стандарта СТБ 34.101, а также порядок использования требований безопасности при сертификации средств реализации этих требований.

При формировании требований безопасности учитывается незавершенность большинства функциональных и гарантийных требований безопасности стандарта СТБ 34.101, ценность информации, архитектура объекта и способы обработки информации.