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.

Для разработки нормативных документов "*Профиль защиты*" и "*Задание по обеспечению безопасности*" предлагается использовать набор детализированных требований безопасности, систематизированных с учетом привязки к объектам информационных технологий и к существующим классам требований СТБ 34.101.

Приводится пример формирования пакетов функциональных и гарантийных требований безопасности.

Описаны подходы при сертификации средств реализации требований безопасности на базе пакетов функциональных и гарантийных требований безопасности.

ФУНКЦИОНАЛЬНЫЕ И ГАРАНТИЙНЫЕ ПАКЕТЫ ТРЕБОВАНИЙ К СРЕДСТВАМ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ

С.К. ТУРБИН, М.А. ТАЛАЛУЕВА

Рассматривается задача формирования требований по управлению безопасностью в виде пакетов требований.

В практике имеются случаи, когда на ранних этапах разработки информационных систем нельзя четко описать объект, угрозы безопасности и на этой основе сформулировать задачи безопасности. В этих случаях целесообразно разрабатывать не профиль защиты (ПЗ), а пакеты функциональных и гарантийных требований.

По существу разработка пакета – первый шаг к созданию некоторого профиля защиты или семейства ПЗ, и к использованию в задании по обеспечению безопасности (ЗБ).

Опыт формирования пакетов весьма ограничен. На сегодняшний день практическими примерами пакетов являются уровни гарантии оценки, определенные в СТБ 34.101.3, которыми следует пользоваться для формирования гарантийных пакетов.

Пакеты, предназначены для многократного использования:

- потребителями в качестве пособия при обосновании требований к средствам управления безопасностью;
- экспертами (испытателями) при проверке соответствия представленных на сертификацию средств управления безопасностью заданным функциональным и гарантийным требованиям безопасности.

Эффект от использования пакетов состоит:

- в уменьшении стоимости разработки ПЗ и (ЗБ);
- в сокращении сроков и объемов работ при разработке ПЗ или ЗБ при выборе или определении требований к средствам управления безопасностью.

КЛАССИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

С.К. ТУРБИН, В.К. ФИСЕНКО

Основными целями защиты информации являются обеспечение ее конфиденциальности, целостности и доступности. Поэтому целесообразно провести классификацию всего множества средств защиты по целевому назначению. С учетом того, что в соответствии с принципом суперпозиции сложная техническая система подразделяется на средства непосредственно исполнительные и средства, поддерживающие эффективное функционирование первых, установлено следующее множество классов средств защиты информации { A_i }:

A_1 — класс средств обеспечения конфиденциальности;

A_2 — класс средств обеспечения целостности;

A_3 — класс средств обеспечения доступности;

A_4 — класс средств контроля (аудита) безопасности;

A_5 — класс средств управления безопасностью.

Задача распределения средств защиты информации из заданного множества $\{S_j\}$ по классам $\{A_i\}$ решается путем логической проверки наибольшего соответствия совокупности признаков целевой направленности средства $(n_{1j},...n_{ij},...n_{Ij})$ классификационным признакам A_i – го класса $(r_{1i},...r_{mi},...r_{mI})$ – $max_{ji}\ (n_{ij} \Lambda\ r_{mi}) => S_j \in A_i$.

ОСНОВНЫЕ НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЯХ

А.В. ПРИБЫЛЬСКИЙ, Т.Г. ТАБОЛИЧ

В условиях рыночной экономики резко обостряется конкурентная борьба между производителями товаров и услуг за потенциальных заказчиков и потребителей. Большинство предприятий РБ пока не занимают лидирующих позиций в этой борьбе на белорусском и зарубежных