ИНФОРМАЦИОННО-СПРАВОЧНАЯ СИСТЕМА ПО СОСТОЯНИЮ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

О. К. Барановский, Е. А. Барсуков, В. В. Скакун

Научно-исследовательский институт технической защиты информации, Минск, Беларусь

Потеря функциональности, заключающаяся в нарушении безопасности информации критически важных объектов (КВО) инфраструктуры государства влияет на состояние его национальной безопасности. В этой связи актуальным является организация государственного учета и контроля информационной безопасности КВО. Достижение цели обеспечивается путем создания информационной системы (ИС) по действующим и создаваемым ключевым системам и объектам (КО) информационно-телекоммуникационной инфраструктуры (ИТИ).

Разработанная ИС предназначена для решения задач наполнения, редактирования, поиска и анализа информации по обеспечению безопасности информации в КО ИТИ, состояния информационной безопасности КВО инфраструктуры государства в целом. База данных (БД) ИС в совокупности описывает:

- КВО инфраструктуры государства;
- субъекты, в чьем владении или распоряжении находятся КВО;
- КО ИТИ, эксплуатируемые на КВО;
- паспорта безопасности КО;
- результаты контроля обеспечения безопасности информации в КО.

ИС состоит из трех независимых подсистем, в соответствии со структурной схемой (рисунок 1):

а) подсистемы администрирования, включающей специальное программное обеспечение (СПО) A1 и центральную БД D1, и предназначенной для добавления и коррекции информации по КО ИТИ в совокупности;

б) распространяемой информационно-справочной подсистемы по действующим и создаваемым КО ИТИ, включающей информационное программное обеспечение (ИПО) A2 и временную БД D2, и предназначенной для поиска и анализа информации;

в) подсистемы аудита, включающей переносимое программное обеспечение (ППО) A3 и локальную БД D3, и предназначенной для

автоматизации процесса внесения новой и коррекции уже имеющейся информации по КО ИТИ на конкретных КВО.

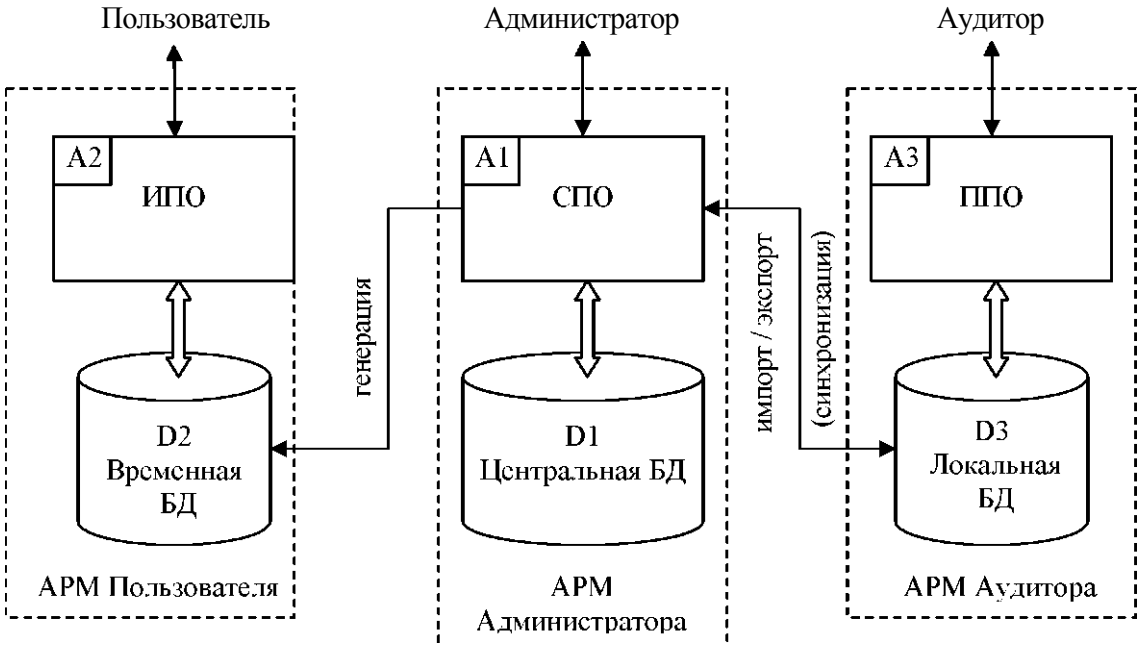

Рис. 1. Структурная схема информационной системы

Центральная БД D1, входящая в подсистему администрирования, физически изолирована от доступа из сетей передачи данных. Предоставление актуализированных данных осуществляется Администратором путем генерации временной БД D2 с учетом прав доступа отдельных Пользователей (уполномоченных органов и организаций). Пользователь, используя временную БД D2 в течение установленного срока ее актуальности, осуществляет поиск информации по заданным критериям, проводит анализ извлекаемых данных. Внесение новых записей и коррекция уже имеющихся по результатам мониторинга или контроля также осуществляется с применением сгенерированных локальных БД D3 (пустых или содержащих записи, требующие актуализации). Аудитор, работая на КВО, вносит изменения в локальную БД D3, которая затем будет синхронизирована с центральной БД D1.

Обеспечение конфиденциальности информации в ИС достигается криптографическим преобразованием данных, авторизацией пользователей и поддержкой различных уровней доступа к ИС путем предоставления программного обеспечения (ПО) для каждого типа пользователей.

При создании ИС реализованы требования к ее запуску на компьютерах под управлением операционных систем (ОС) Windows и Linux, простоты инсталляции, настройки и администрирования отдельных ее частей. ИС спроектирована как кроссплатформенная клиент-серверная система. Разработка ПО ИС велась в операционной системе Windows. В ОС Linux проводилось окончательное тестирование и исправление неточностей, связанных со спецификой ОС и компиляторов. Для обеспечения переносимости исходного кода ПО между ОС использовалась библиотека Qt, позволяющая избавиться от необходимости прямого использования API конкретной ОС.

Унифицированный графический интерфейс ИС состоит из нескольких фреймов доступа к отдельным таблицам или к специально созданным представлениям БД, соединяющим воедино данные из нескольких таблиц. Основное окно пользователя построено таким образом, чтобы при выделении ключевого объекта в главном фрейме происходило автоматическое выделение записей в связанных таблицах и представлениях. Дополнительная информация доступна через справочники, вызываемые через пункты главного меню. Защита данных от случайного или непреднамеренного изменения реализована путем создания отдельных форм для редактирования данных.

Для сокращения числа справочников и форм применена технология "master-detail", что дает возможность просмотра либо редактирования основной таблицы и нескольких подчиненных в одном окне с автоматической установкой внешних ключей в необходимые значения.

Ввиду того, что некоторые объекты имеют сложную иерархическую структуру, при реализации которой потребовалось бы выделение отдельной таблицы для каждого уровня иерархии или введение рекурсивной связи, для снижения сложности структуры данных и повышения универсальности предложено хранить параметры таких объектов в таблицах, в общем случае имеющих поля: "название параметра", "тип параметра", "значение параметра". Такой подход позволяет реализовывать структуры произвольной сложности без потери информационной нагрузки данных.

Эксплуатация ИС позволяет автоматизировать процессы учета, обеспечения мониторинга и контроля информационной безопасности КВО инфраструктуры государства.