С.В. Остах, М.Е. Леонович

ЗАЩИЩЕННОСТЬ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ БЕЗОПАСНОСТИ

Переход к современным компьютерным технологиям ставит задачу создания общей автоматизированной информационно-управляющей системы безопасности потенциально опасных объектах (АИУСБ ПОО). АИУСБ ПОО должна включать в себя распределенную базу данных, диалоговую систему рекомендаций, оптимизирующих действия в условиях чрезвычайных ситуаций (ЧС), многоуровневый аналитический комплекс.

АИУСБ ПОО строится на единой структурной, конструктивно-технологической и электронной базе, имеет унифицированное системное программное обеспечение и гибкий состав подключаемых программно-аппаратных комплексов.

АИУСБ ПОО выполняется на базе вычислительной техники как распределенный децентрализованный комплекс, компоненты которого связаны единой информационно-управляющей сетью в соответствии с функциональной структурой автоматизированной системой управления производством.

Следует также отметить, что в последние годы АИУСБ ПОО интегрируются с автоматизированными системами, распределяющими задачи по управлению ликвидацией последствий крупных ЧС между специализированными научными центрами с использованием сети Интернет.

Взаимозависимость и уязвимость автоматизированных систем обуславливают необходимость создания систем информационной безопасности в составе каждой АИУСБ ПОО.

Постоянно меняющиеся угрозы и способы их реализации не позволяет заранее предусмотреть все возможные варианты систем безопасности и ограничиться фиксированным набором мер защиты [1]. Поэтому нужна концепция обеспечения заданного уровня защищенности от возможных угроз, представляющая собой систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Разработка концепции и политики информационной безопасности позволяет формализовать комплекс организационно-административных, технических и технологических мер по предотвращению угроз разрушения АИУСБ ПОО, уничтожения либо утечки информации, а также устранению их последствий.

Разработка такого рода концепций должна проводиться на этапе формирования информационной модели организации при проектировании автоматизированных систем управления производством.

Для обоснования предварительной конфигурации аппаратных и про-

граммных средств АИУСБ ПОО проводится оценка потенциальных территориальных и информационных рисков, связанных с реализацией угроз безопасности.

Надежная защита от реализации активных угроз может быть обеспечена только эффективными методами блокирования несанкционированного доступа, технологического аудита, а также контроля и восстановления эталонного состояния АИУСБ ПОО.

Концептуальная модель защищенности АИУСБ ПОО включает в себя несколько уровней безопасности:

- каналов передачи информации;
- от несанкционированного доступа в автоматизированную систему;
- от несанкционированного доступа к информации, хранящейся в базах данных;
- информации от потерь в результате повреждения технических средств.

Подсистема информационной безопасности АИУСБ ПОО должна обеспечивать выполнение следующих функций:

- выделение информации, подлежащей защите;
- охват всех видов носителей информации;
- сохранность всех видов носителей и информации на них;
- выявление и документирование факта утечки информации;
- выявление лиц, причастных к этому нарушению;
- возможность пассивного и активного пресечения возникшего нарушения, а в дальнейшем - предупреждение нарушения.

С учетом этого представляется целесообразной интеллектуализация системы обеспечения информационной безопасности, обеспечивающей управление средствами защиты АИУСБ ПОО.

Литература

1. Гинзбург В.В., Качанов С.А. и др. Безопасность информационных систем в условиях глобализации. –М.: Радио и связь, 2003 . –249 с.