ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМЫ РАЗВЕДКИ ВОЗДУШНОГО ПРОСТРАНСТВА

С.В. Потетенко, В.С. Жуковский, И.Л. Семченко

Обеспечение информационной устойчивости АСУ ПВО требует соблюдения информационной безопасности системы разведки воздушного пространства, основными компонентами которой являются: конфиденциальность, доступность и целостность.

Достижение требуемого уровня качества каждой компоненты решает задачу информационной безопасности в целом.

Защите подлежит информация, передаваемая по каналам связи и хранящаяся на энергонезависимых носителях, т.к. безопасность информации в оперативной памяти обеспечивается организационными мерами. Условно, по требуемым значениям компонент безопасности, информацию целесообразно классифицировать по критериям: по типу объекта (воздушный, средство разведки, потребитель); по динамике изменения (динамическая, статическая); по степени важности.

Требования к конфиденциальности информации, т.е. сохранению ее в тайне и регламентации границ использования, определяется сроком актуальности. Конфиденциальность достигается криптографическими методами, причем стойкость шифрования должна гарантированно обеспечивать срок взлома ключа, превышающий срок актуальности информации.

Требования к доступности, т.е. своевременный и беспрепятственный доступ пользователей, определяются динамическими правами доступа пользователей, формируемыми на основе их статических и динамических свойств, в качестве которых используются функциональное назначение элемента системы, его тактико-технические характеристики, текущее местоположение, состояние и производимые действия.

Требования к целостности, т.е. существованию информации в неискаженном и подлинном виде, определяются ее контекстом. Обеспечиваются применением хеширования для информации о наземных объектах и статической информации о воздушных объектах. Динамическая информация о воздушных объектах имеет малое время актуальности и высокую автокорреляцию, что позволяет ограничиться применением контрольных кодов с малой избыточностью только на этапе передачи.

Для каждого вида передаваемой и хранимой информации определены требования по конфиденциальности, доступности и целостности, методы их обеспечения и разработаны рекомендации по практической реализации в перспективных образцах ВВТ.