

ВОЗМОЖНОСТИ РЕАЛИЗАЦИИ СИСТЕМЫ КОНТРОЛЯ САНКЦИОНИРОВАННОГО ПРИМЕНЕНИЯ РАКЕТНОГО ОРУЖИЯ

В. В. Сербин, В. В. Сухой, И. В. Михайлова

Государственное предприятие «Конструкторское бюро «Южное»
Украина, г. Днепр
info@yuzhnoye.com

Создание автоматизированных систем управления для Вооруженных сил Украины является сейчас самой востребованной разработкой для специализированных научных организаций. Здесь необходимо решить достаточное количество сложных проблем, таких как, например, выбор оптимальных характеристик средств связи и обеспечение необходимых показателей стойкости управления. Отдельной важной проблемой при создании автоматизированных систем управления ракетными подразделениями является обеспечение безопасности управления и применения ракетного комплекса. Рассмотрен общий подход к реализации системы контроля санкционированного применения ракетного комплекса.

Ключевые слова: автоматизированная система управления, ракетный комплекс.

При создании новых образцов ракетного вооружения, особенно ракетных комплексов оперативно-тактического назначения, следует учитывать угрозы различного характера, возникающие в современных условиях ведения боевых действий:

- угрозы, которые характерны для военно-политических условий применения ракетного комплекса;
- угрозы, которые характерны для различных оперативных условий применения ракетного комплекса;
- угрозы кумулятивные, которые характерны одновременно для обеих вышеприведенных категорий угроз.

Одной из самых проблематичных является угроза захвата самоходных пусковых установок ракетного комплекса разведывательно-диверсионными группами противника или незаконными террористическими формированиями с целью применения ракетного оружия в своих целях.

Целью настоящей работы является выбор методов обеспечения безопасности для реализации системы контроля санкционированного применения ракетного оружия с требуемым уровнем безопасности применения ракетного комплекса в любых условиях оперативной и военно-политической обстановки.

Под несанкционированным применением ракетного оружия следует понимать:

- несанкционированное выполнение приказа на пуск. Данное действие может возникнуть вследствие выполнения личным составом самоходной пусковой установки процедур и действий, приводящих к запуску двигательной установки ракеты или запуску устройства минометного старта, приводящего к сходу ракеты с пускового устройства;
- пуск ракеты по незапланированной цели. Данное действие может возникнуть вследствие ввода координат цели, которые отсутствуют в заранее сформированной базе данных целей либо которые отсутствуют в приказе на пуск, поступившем с верхних звеньев управления;
- отмену пуска ракеты личным составом самоходной пусковой установки. Данное действие может возникнуть вследствие выполнения личным составом самоходной пусковой установки несанкционированных действий и процедур, приводящих к отмене запуска ракет и невыполнению поставленной боевой задачи.

Анализ оперативных условий применения ракетного комплекса позволяет сформулировать три класса возможных методов обеспечения безопасности контура боевого управления — организационные (режимные), алгоритмические и программно-технические.

В основу использования организационных (режимных) методов защиты положен принцип выполнения личным составом самоходной пусковой установки специальных процедур — использование специальной документации, доклады о состоянии и боеготовности ракетного оружия, организа-

ция дежурства и охраны с целью исключения случайного или преднамеренного доступа неуполномоченных лиц (нарушителей) к аппаратуре управления ракетными пусками.

Алгоритмический метод защиты базируется на применении системной защиты от попыток формирования и ввода в аппаратуру управления несанкционированных приказов и команд управления, включая несанкционированный доступ к информации боевого управления. Основой алгоритмической защиты является концепция использования шифров. Данный метод возможно реализовать с помощью аппаратуры криптографической защиты информации, при наличии которой в каналах приема/передачи информации гарантируется «санкционирование» приказа/команды, полученной с высшего звена управления.

Программно-технические методы защиты предусматривают использование средств, позволяющих предотвратить факты несанкционированного пуска ракет, возникающие вследствие проведения случайных или преднамеренных (в т. ч. нештатных или ошибочных) действий личного состава. К основным из них относятся:

— использование личным составом самоходной пусковой установки различных атрибутов разграничения доступа к аппаратуре боевого управления (например, электронных идентификаторов полномочий должностных лиц типа USB Flash Key);

— использование электромеханических замков, с помощью которых контролируется доступ к аппаратуре боевого управления;

— использование специальных устройств типа «ключ/кнопка», с помощью которых обеспечивается алгоритм совместных действий личного состава для разблокирования электрических цепей прохождения сигналов на пуск ракеты.

Приведенный анализ методов обеспечения безопасности контура боевого управления показывает наличие ярко выраженной функциональной взаимосвязи алгоритмических и программно-технических методов. Реализация данного подхода предполагает симбиоз применения средств защиты от несанкционированного доступа к информации, хранящейся в контуре боевого управления, средств криптографической защиты информации в каналах получения боевых приказов и средств обеспечения совместных действий личного состава типа «ключ/кнопка», которые размещаются на самоходных пусковых установках и звеньях управления ракетным подразделением.

Предлагаемое решение по защите ракетного комплекса от несанкционированного применения позволяет реализовать:

— необходимую степень взаимной интеграции логики функционирования специальных алгоритмов защиты информации с внутрисистемной логикой алгоритмов боевого управления;

— идеологическую целостность и унификацию состава аппаратуры боевого управления;

— непрерывность и автономность функционирования контура боевого управления;

— вариативность логики функционирования, т. е. адаптация к типу и модификации различных защищаемых объектов;

— ограничения доступа к аппаратуре боевого применения ракетного оружия со строгим соблюдением ответственности личного состава за применение вооружения на всем протяжении его жизненного цикла.

Рассмотренный общий подход к реализации системы контроля санкционированного применения ракетного оружия позволяет обеспечить целостный подход и системность решения задачи защиты ракетного вооружения, начиная с этапа проектирования, что является основным критерием надежной и безопасной эксплуатации ракетных комплексов впоследствии.

V. V. Serbin, V. V. Sukhyy, I. V. Mikhaylova

Possibilities for the implementation of the control system for the authorized use of missiles

The development of automated control systems for the Armed Forces of Ukraine is currently the most popular development area for specialized scientific organizations. To deal with this task, one needs to face an ample amount of complex problems, e.g. choosing the optimal characteristics of communication equipment, providing the necessary indicators of management stability. Another important problem in the development of automated control systems for missile units is ensuring security for management and application of the missile system. The paper considers a general approach to the implementation of the control system for the authorized use of missile systems.

Keywords: automated control system, missile system.