

УДК: 621.325:621.391

В.Н. Шлокин¹, С.В. Малахов¹, А.Г. Снисаренко¹, А.Л. Гостев¹,
С.Г. Вдовенко², А.М. Присяжный²¹Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков²Центральное управление защиты информации и криптологии ГШ ВС Украины, Киев

ОБЩЕСИСТЕМНЫЕ ВОПРОСЫ САНКЦИОНИРОВАНИЯ ПРИМЕНЕНИЯ РАКЕТНЫХ КОМПЛЕКСОВ СУХОПУТНЫХ ВОЙСК

Рассмотрены общие положения проблематики санкционирования применения ракетных комплексов Сухопутных войск.

Ключевые слова: ракетный комплекс, угрозы, несанкционированные действия, передача полномочий, совместные действия.

Введение

В процессе проектирования и создания новых образцов ракетных комплексов (РК), а также модернизации РК, находящихся на вооружении Сухопутных войск (СВ), наряду с решением ряда традиционных задач (анализ, выбор, обоснование и внедрение принимаемых технических решений), участники данного процесса – представители промышленности и военно-научного сопровождения, так или иначе сталкиваются с необходимостью обеспечения требуемого уровня легитимности применения РК.

В общем случае, уровень контроля процедур инициализации и выполнения особо важных команд боевого управления и пусковых циклограмм РК является комплексным критерием, учитывающим степень сложности принятых технических решений и реализации процедур обслуживания и боевого применения РК, а также способность противостоять воздействию угроз различного характера.

При этом, одним из важнейших элементов РК СВ является его автоматизированная система управления (АСУ), технические характеристики которой в значительной мере определяют требуемый уровень безопасности применения РК.

Ввиду особой роли АСУ РК, выступающей связующим звеном между обслуживающим персоналом и оружием, рассмотрение вопросов обеспечения процедур легитимного боевого применения РК СВ и передачи (делегирования) полномочий управления между его звеньями управления является важной задачей.

Помимо этого, своевременное согласование позиций представителей промышленности и Министерства обороны по указанным вопросам в значительной мере позволяет нивелировать возможные разногласия в сути конечной цели решаемых задач – санкционирования процесса применения оружия. В противном случае возможно повторение организационных и системных ошибок, аналогичных описанным в [1].

Целью публикации является дальнейшее развитие проблематики санкционирования (легитимизации) применения РК СВ и уточнение некоторых концептуальных и методологических положений в соответствии с современными взглядами на ведение вооруженной борьбы и последними технологическими тенденциями.

Для достижения поставленной цели представленный материал изложен в рамках двух взаимосвязанных структурно-логических блоков:

– обобщенный ретроспективный обзор проблематики защиты от несанкционированных действий и несанкционированных пусков ракет (НСД/НСП) в различных условиях войсковой эксплуатации и применения РК СВ;

– краткое рассмотрение общесистемных вопросов, связанных с функциональной концепцией системы защиты от НСД/НСП и ее реализацией в различных элементах РК СВ.

В этой связи важно подчеркнуть, что ввиду значительного многообразия исходных условий и вариантов технической реализации системы защиты, предложенный к рассмотрению материал следует рассматривать, как носящий обзорно-концептуальный характер, определяющий основные категории данной проблематики и направления реализации возможных технических решений в рамках создания систем и средств защиты от НСД/НСП в РК СВ.

Актуальность рассматриваемых вопросов обусловлена произошедшей за последнее десятилетие эволюцией общего представления специалистов о функциональном облике высокоточных средств огневого поражения вообще, и РК СВ в частности, что нашло свое логичное продолжение в качественном изменении вновь создаваемых образцов и систем РК СВ [2 – 6] для которых свойственны:

– высокая степень автоматизации и информатизации процессов управления;

– возможность обеспечения одновременного дистанционного управления значительным количеством боевых единиц;

- высокая оперативность применения и малое время реакции с момента формирования пусковых команд;
- возрастание требований к уровню подготовки номеров боевых расчетов (персонала);
- информационная интеграция с другими (внешними) системами и комплексами;
- увеличение дальности применения ракетного оружия и улучшение их точностных характеристик при значительной вариативности применяемого боевого оснащения ракет.

Основной материал

В общем случае рассмотрения проблематики защиты от НСД/НСП диктует необходимость проведения соответствующего анализа угроз, обуславливающих возникновение предпосылок совершения НСД/НСП в различных условиях эксплуатации и применения РК СВ. В свою очередь, задачу анализа возможных угроз необходимо решать, опираясь на результаты систематизации опыта войсковой эксплуатации и боевого применения известных образцов РК, с одной стороны, и аналитического прогноза основных тенденций развития РК СВ, с другой стороны.

По нашему мнению, в перспективных РК СВ комплексные системы защиты от НСД/НСП по составу решаемых ими задач и специфике интеграции специальных устройств в состав оборудования различных элементов РК, идентичны как для РК с обычным, так и с высокоточным оснащением. При этом, для высокоточных РК основные отличия в реализации подобных систем заключаются в расширении перечня постоянно контролируемых параметров основных систем РК, что реализуется путем изменения конфигурации специального программного обеспечения (СПО) системы защиты от НСД/НСП, а также расширения качественного и количественного состава датчиков и исполнительных элементов системы защиты.

Подобное сходство систем защиты, реализуемых в РК СВ с обычным и высокоточным оснащением, обусловлено крайне узкой целевой направленностью подобных систем, в любом случае решающих две основные задачи:

1. санкционирование применения оружия, т.е. легитимное проведение пусков ракет;
2. защита от несанкционированных действий обслуживающего персонала РК и третьих лиц при реализации особо важных процедур управления (например, при передаче органами управления верхних звеньев части своих полномочий нижним звеньям по управлению ракетными формированиями);
3. защита от влияния посторонних факторов воздействия.

При этом, под несанкционированным пуском (НСП) ракет при отсутствии соответствующих на это санкций, получаемых, как правило, с верхних

звеньев управления (ВЗУ), будем понимать:

- несанкционированный запуск двигательной установки ракеты;
- несанкционированный запуск устройства минометного старта, приводящий к сходу ракеты с пускового устройства;
- пуск ракеты по незапланированной цели.

Тогда под несанкционированными действиями (НСД) персонала при эксплуатации и боевом применении РК СВ будем понимать действия, заключающиеся в реализации случайного или умышленного информационно-технического воздействия на аппаратуру АСУ РК и пусковые цепи самоходных пусковых установок (СПУ), которые способны привести к:

- изменению заданного/текущего технического состояния и состава соответствующих (охваченных функциональным контролем со стороны системы защиты от НСД/НСП) программно-аппаратных средств звеньев управления;
- изменению степени боевой готовности ракетных формирований;
- изменению иерархического статуса командных пунктов (пунктов управления) и/или текущих полномочий должностных лиц;
- переприцеливанию ракет, в т.ч. к изменению значений установок целеуказаний.

С целью наиболее полного освещения рассматриваемой проблематики изначально важно обратить внимание на существование следующих принципиальных аспектов, характерных для различных условий применения РК СВ:

- военно-политические условия, при которых происходит или планируется войсковая эксплуатация и боевое применение РК. При этом процессы, входящие в сферу компетенции военно-политических условий, характеризуются статичным или медленно меняющимся характером изменения возможных состояний;

- оперативные условия применения РК СВ. Для данной группы свойственны значительный полиморфизм и высокая динамика изменения возможных состояний.

По результатам анализа специфики условий эксплуатации и особенностей боевого применения РК СВ можно сформировать три группы угроз возникновения предпосылок совершения НСД/НСП:

- угрозы, характерные для различных военно-политических условий применения (эксплуатации) РК СВ;
- угрозы, характерные для различных оперативных условий применения РК СВ;
- угрозы кумулятивного характера, свойственные одновременно для двух рассмотренных выше категорий.

Парирование угроз последней группы обеспечивает наиболее адекватный, с точки зрения нейтра-

лизации их последствий, эффект, включая и экономическую сторону вопроса, которая учитывает баланс между вероятностью возникновения угрозы, технической сложностью ее парирования и необходимыми для этого ресурсными затратами.

С точки зрения парирования угроз, использование вышешприведенного порядка их структурирования позволяет проявить наиболее критичные особенности, характерные для различных условий применения РК, и создает достаточную основу для формирования предложений по составу и содержанию мероприятий, направленных на предотвращение последствий этих угроз. При этом, принципиально важно подчеркнуть то, что специфика вопросов защиты от НСД/НСП требует их безусловного распространения не только на этап непосредственно боевого применения РК, но и на весь его жизненный цикл. Выполнение данного требования по своей сути декларирует необходимость обеспечения заданного уровня легитимизации боевого применения и безопасной эксплуатации РК СВ в любых складывающихся условиях обстановки.

Наряду с вышесказанным необходимо отметить тот факт, что вопросы реализации мероприятий по защите от НСД/НСП де-факто имеют свои техническую и юридическую стороны. Так, с технической точки зрения, выполнение мероприятий по защите от НСД/НСП имеют своей целью комплексное обеспечение функций блокирования любых возможностей по осуществлению несанкционированных пусков ракет и несанкционированной реализации заданного перечня особо важных процедур управления оружием и войсками.

Юридическая же сторона вопроса находится в плоскости обеспечения гарантий на реализацию решений по применению оружия строго заданному кругу лиц, с одной стороны, и четкой регламентацией фактической ответственности за принятые ими решения на применение оружия и управление войсками, с другой стороны.

Таким образом, помимо случаев, непосредственно связанных с применением РК по назначению, область реализации мероприятий по защите от НСД/НСП должна быть расширена на следующие основные этапы и процедуры жизненного цикла РК СВ:

- при проведении летно-конструкторских испытаний (ЛКИ) новых или модернизированных образцов ракет или РК на испытательных полигонах;
- при вводе в эксплуатацию РК (в т.ч. опытная эксплуатация);
- при проведении учебно-боевых пусков в ходе проведения учений;
- при проведении регламента и доработок программно-аппаратных средств АСУ командно-штабных машин (КШМ) и СПУ, а также аппаратуры пусковых цепей СПУ;

- при поиске и устранении неисправностей и ремонтно-восстановительных работах на средствах АСУ КШМ, СПУ и пусковых цепях СПУ, а также аппаратуре и антенных устройствах средств связи (СС) КШМ и СПУ;

- при опросах состояния аппаратуры тракта боевого управления, кодоблокирующих устройств (КБУ) КШМ и СПУ, а также пусковых цепей СПУ (включая отдельные бортовые системы ракет при наличии соответствующих технических возможностей);

- в процессе приема и передачи контрольных, учебных или технологических команд и автоматических донесений по тракту боевого управления РК, а также по пусковым цепям СПУ;

- в процессе делегирования (передачи) полномочий по формированию пусковых команд/приказов на проведение пусков ракет органам управления (ОУ) других звеньев управления;

- в процессе делегирования (передачи) полномочий по управлению ракетными формированиями ОУ других звеньев управления;

- при нахождении КШМ и СПУ на хранении в парках и арсеналах (при необходимости);

- при перевозке КШМ и СПУ различными видами транспорта (при необходимости).

Анализ возможных военно-политических условий [7], при которых планируется войсковая эксплуатация и применение по назначению РК СВ Украины, позволяет сформировать следующий перечень их возможных состояний:

- мирное время (осуществление пусков в ходе проведения плановых учений или ЛКИ);

- угрожаемый период (разворачивание и маневр ракетных формирований в назначенном им позиционном районе, несение боевого дежурства, проведение учебно-боевых стрельб с целью демонстрации силы);

- начало локальной/региональной войны или вооруженных конфликтов различной интенсивности (действия в составе Объединенных сил быстрого реагирования или других межвидовых группировок войск с целью локализации возникшего военного конфликта и недопущения его дальнейшей эскалации);

- отражение широкомасштабной агрессии (в составе межвидовых группировок войск);

- участие в составе многонациональных контингентов в конфликтоопасных регионах (выполнение задач проекции силы и поддержки действий коалиционных сил).

Очевидно, что с точки зрения анализа причинно-следственных связей, каждое из пяти выше перечисленных состояний обуславливает собой существование характерного для него спектра возможных угроз возникновения предпосылок совершения НСД/НСП, которые в той или иной мере перекли-

каются с угрозами, свойственными для других военно-политических условий.

Соответственно, анализ оперативных условий, при которых планируется войсковая эксплуатация РК и предполагается их применение по назначению, позволяет сформулировать перечень обязательных для рассмотрения факторов, соответствующих данной категории условий, таких как:

- особенности построения боевых порядков, характерных для РК различных типов оснащения;
- особенности организации боевого управления при выполнении задач по назначению;

– особенности работы номеров боевых расчетов КШМ и СПУ при выполнении задач по назначению.

Учитывая объемность материалов анализа возможных состояний и факторов, характерных для указанных выше условий, а также ограничения, накладываемые рамками публикации, специфику угроз, свойственных для военно-политических и оперативных условий применения РК СВ, рассмотрим на примере основных составляющих блока кумулятивных угроз (табл. 1), парирование которых, обеспечивает наибольший практический эффект.

Таблица 1

Основные составляющие блока кумулятивных угроз

№ п/п	ОСНОВНОЙ СОСТАВ КУМУЛЯТИВНЫХ УГРОЗ	
	УГРОЗЫ ОРГАНИЗАЦИОННОГО ХАРАКТЕРА	УГРОЗЫ ТЕХНИЧЕСКОГО ХАРАКТЕРА
1	– неоднократные, подряд следующие нарушения заданного порядка реализации совместных действий номерами расчетов звена управления;	– возникновение программных, программно-аппаратных сбоев в работе КБУ, аппаратуры трактов боевого управления и пусковых цепей СПУ или нарушение режимов их электропитания;
2	– неоднократные подряд следующие попытки подбора пароля, предоставляющего право работы на соответствующей аппаратуре звена управления (<i>т.е. попытки неправомерной аутентификации</i>);	– нарушение функционирования аппаратуры трактов боевого управления вследствие их подавления и/или навязывания ложной информации.
3	– неправомерная передача полномочий (права боевой работы на аппаратуре звена управления) между номерами боевого расчета звена управления, а также утрата или повреждение материальных атрибутов разграничения доступа к соответствующей аппаратуре звена управления;	
4	– умышленные/неумышленные действия, заключающиеся в попытках изменения установленных ВЗУ режимов функционирования аппаратуры данного звена управления;	
5	– умышленные/неумышленные действия, заключающиеся в попытках нелегитимной передачи органам управления нижних звеньев управления (НЗУ) полномочий по формированию ими пусковых команд/приказов или управлению элементами других звеньев управления;	
6	– выполнение действий под принуждением;	
7	– несанкционированный с ВЗУ набор и ввод в систему управления заданного перечня особо важных приказов/команд;	
8	– неавторизованное изменение состава аппаратуры и программных средств системы управления КШМ и СПУ, а также пусковых цепей СПУ;	
9	– попытки неправомерного отключения, демонтажа или нарушения целостности элементов системы защиты от НСД/НСП;	
10	– выдача в каналы связи контрольной информации при проведении технического обслуживания аппаратуры звена управления, в т.ч. несанкционированный выход контрольной информации по техническим каналам утечки посредством побочных электромагнитных излучений.	

При этом следует иметь в виду, что представленный перечень кумулятивных угроз возникновения предпосылок совершения НСД/НСП является результатом группировки, обобщения и взаимного поглощения соответствующих видов угроз, характерных для указанных выше условий применения и эксплуатации РК различных типов.

Так как в иерархических системах управления современных РК СВ [3, 4] на различных этапах их циклов боевого управления задействованы как тех-

нические средства, так и обслуживающий персонал (номера боевых расчетов), то очевидно, что в качестве источников возникновения НСД/НСП необходимо рассматривать и действия номеров боевых расчетов (человеческий или организационный фактор), и технические средства системы управления РК и пусковых цепей СПУ (технический фактор возникновения НСД/НСП).

В контексте анализа данных, представленных в табл. 1, важно подчеркнуть, что последствия от реа-

лизации несанкционированных действий или несанкционированных пусков, вне зависимости от причины, т.е. угрозы, их породившей, являются в равной степени недопустимыми, поэтому система предотвращения НСД/НСП, как минимум, должна обеспечить паритетную защиту от всех видов кумулятивных угроз.

При этом общий защитный функционал обеспечивается комбинированием технических и организационных мер (рис. 1), где технические меры, безусловно, являются основными и, в конечном итоге, определяют фактический уровень защиты РК для выбранной функциональной концепции системы.



Рис. 1. Инфографика организации защиты от НСД/НСП

Таким образом, решение задачи формирования требований к функциям и перечню задач системы защиты от НСД/НСП должно опираться на результаты анализа и систематизации угроз, характерных для конкретных типов РК. В результате этого создаются необходимые условия для построения адекватной стратегии защиты, уточнения ее основных принципов, и, как следствие, определения требуемого состава и комбинации соответствующих методов и способов парирования всей совокупности актуальных угроз.

В общем случае, применительно к специфике РК СВ, можно выделить три основных класса методов защиты (рис. 1):

- организационные (режимные);
- алгоритмические;
- программно-технические.

В основу использования организационных (режимных) методов защиты положен принцип адаптивной преемственности опыта войсковой эксплуатации и боевого применения РК различных типов. При этом, основные требования к данным методам защиты в значительной мере определяются положениями профильного боевого устава, а также соответствующими приказами и распоряжениями должностных лиц оборонного ведомства. В качестве примера основных организационных методов можно привести следующие:

- комплектация КШМ и СПУ специальной документацией;
- выполнение особо важных операций боевого управления с использованием номерами боевых расчетов алгоритма совместных действий;
- реализация в циклах управления системы периодических докладов о состоянии и боеготовности звеньев управления;
- организация дежурства с целью исключения случайного или преднамеренного доступа неуполномоченных лиц к аппаратуре звеньев управления.

Алгоритмические (общесистемные) методы базируются на идеологии системной защиты от попыток формирования и ввода в систему управления несанкционированных приказов и команд управления, включая несанкционированный доступ к информации боевого управления. Основой алгоритмической защиты является концепция использования специальных чисел – шифров (кодов или паролей), в основных чертах схожей с концепцией использования электронных подписей. Порядок формирования таких шифров определяется специально уполномоченной на это службой.

Основная цель использования шифров – управление работой КБУ, играющего главную роль в реализации функций защиты трактов боевого управления КШМ и СПУ, а также пусковых цепей СПУ при прохождении по ним пусковых приказов и других

особо важных команд управления (например, на перевод звена управления из одной степени готовности в другую). При этом значения шифров передаются "сверху-вниз" и служат для нижних звеньев управления (НЗУ) подтверждением их полномочий на проведение пусков или выполнение особо важных команд управления.

В упрощенном виде процесс управления работой КБУ выглядит следующим образом: в случае совпадения принятого с ВЗУ значения шифра с его эталоном, хранящемся в КБУ, последнее «санкционирует» выполнение данным звеном управления приказов/команд, полученных с ВЗУ. В противном случае КБУ блокирует выполнение поступивших приказов/команд, а на ВЗУ, в случае необходимости, может быть отправлено соответствующее донесение.

В случае ввода приказов/команд (в т.ч. значений шифра) непосредственно на звене управления в ситуации, когда в результате ввода значений шифра получены отрицательные результаты их сравнения с эталонным значением, КБУ производит блокировку данного звена управления. При этом на ВЗУ передается автоматически сформированное донесение, служащее для органов управления ВЗУ сигналом, свидетельствующим о зафиксированном факте совершения НСД на конкретном звене управления. Дальнейшие процедуры по разблокировке данного звена управления могут быть произведены только представителем специально уполномоченной службы с использованием сервисного пульта путем введения с него в КБУ команд разблокировки.

Кроме того, к группе алгоритмических методов предотвращения НСД/НСП следует отнести и практику использования метода накопления так называемой «пусковой ситуации». В соответствии с ним осуществление пусков любым из звеньев управления возможно только при выполнении заданного перечня обязательных логических условий, связанных с анализом текущего состояния информационных процессов и параметров системы управления РК, детальное рассмотрение которых, выходит за рамки данной публикации. При этом факт ввода непосредственно на звене управления информации, относящейся к «пусковой ситуации», должен сопровождаться автоматической передачей соответствующих донесений на ВЗУ.

Также, в рамках рассмотрения специфики алгоритмических методов, необходимо отметить некоторые принципиальные особенности использования выносной консоли управления пуском (ВКУП), являющейся удаленным терминалом автоматизированного рабочего места (АРМ) СПУ и позволяющей проводить пуски ракет в условиях непосредственного отсутствия расчета на СПУ. Как правило, в штатном положении, ВКУП включена в информационные цепи АСУ СПУ, целостность которых постоянно контролируется КБУ, а для извлечения ВКУП из монтажной стойки требуется реализация алгоритма

выполнения совместных действий, чем и обеспечивается легитимность ее использования.

Программно-технические методы защиты от НСД/НСП предусматривают использование средств, позволяющих предотвратить возможные негативные последствия, возникающие вследствие проведения случайных или преднамеренных (в т.ч. нештатных или ошибочных) действий обслуживающего персонала. К основным из них следует отнести:

- использование номерами боевых расчетов КШМ и СПУ различных атрибутов разграничения доступа к осуществлению функций боевого управления (например, электронных идентификаторов полномочий должностных лиц типа USB Flash Key или персональных ключей к электромеханическим замкам (ЭМЗ) пультов АРМ КШМ и СПУ и др.);

- внедрение практики использования сменных паролей (например, PIN-кодов) на период выполнения конкретных задач;

- автоматическое документирование действий номеров боевых расчетов при реализации ими заданного перечня особо важных функций (процедур) управления;

- применение механизма автоматически формируемых и передаваемых на ВЗУ донесений о фиксируемых фактах НСД/НСП;

- техническое обеспечение выполнения алгоритма совместных действий при вводе в систему управления РК информации, относящейся к категории особо важных процедур управления, в том числе при проведении пусков ракет. В данном случае следует отметить наличие ярко выраженной функциональной взаимосвязи организационных и программно-технических методов (заштрихованная область на рис. 1), что подчеркивает комплексный характер защиты от НСД/НСП.

Переходя к рассмотрению особенностей технической реализации системы защиты от НСД/НСП, входящей в состав оборудования КШМ и СПУ (рис. 2), следует обратить внимание на совпадение их концептуальных архитектур, что свидетельствует о возможности потенциально высокой степени унификации реализуемых в них стратегий защиты. При этом имеющиеся отличия обусловлены разницей в составе функциональных задач, решаемых персоналом КШМ и задач, решаемых расчетами СПУ.

Так, например, с точки зрения разработчика СПО для КБУ КШМ, важнейшими функциональными задачами, которые необходимо учесть в процессе разработки соответствующих алгоритмов, являются:

- поддержка возможностей дистанционного управления проведением пусков ракет любой из подчиненных СПУ (включая режим управления через инстанцию);

- избирательная передача части имеющихся полномочий по управлению войсками (для ОУ) и/или применение оружия соответствующим должностным лицам НЗУ. При этом следует подчерк-

нуть, что необходимость подобной передачи полномочий носит случайный характер и реализуется, сообразно складывающейся оперативной обстановке. Например, при предоставлении ОУ НЗУ полно-

мочий на самостоятельное принятие решения по применению оружия в зависимости от складывающейся в зоне их ответственности обстановки, без отдельной на это санкции с ВЗУ.

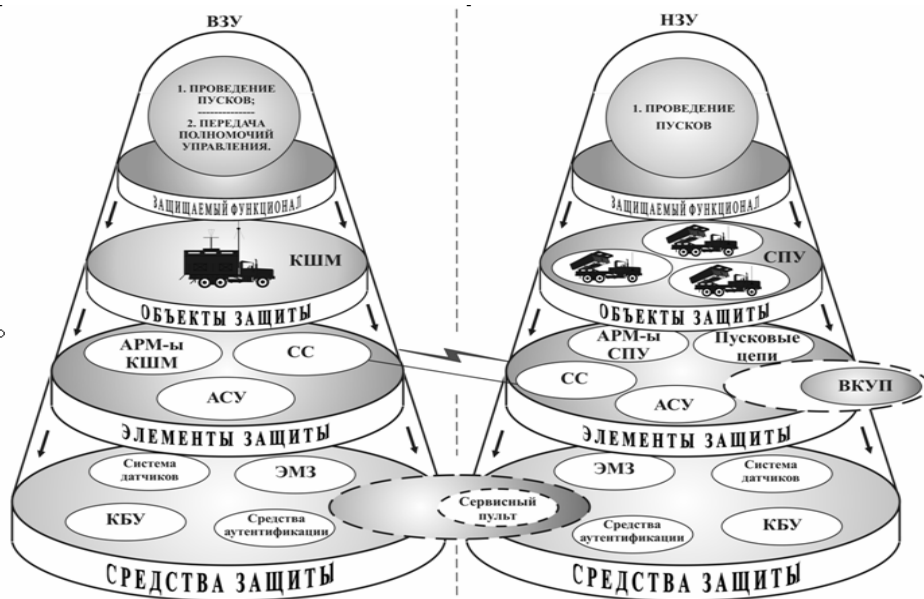


Рис. 2. Упрощенная архитектура построения защиты от НСД/НСП основных элементов РК СВ

Соответственно, с точки зрения разработчика СПО для КБУ СПУ, такой задачей является поддержка режима автономного пуска ракет (в т.ч. с применением ВКУП).

Существование выше указанных особенностей находит свое продолжение в различных версиях СПО для кодоблокирующих устройств КШМ и СПУ, что обусловлено различиями в логике их функционирования и соответствующем изменении состава контролируемых параметров основных подсистем КШМ и СПУ (рис. 3), охваченных функциональным контролем со стороны системы защиты от НСД/НСП. При этом использование модульного принципа построения СПО КБУ позволяет:

- обеспечить необходимую степень взаимной интеграции логики функционирования специальных алгоритмов защиты с внутрисистемной логикой алгоритмов боевого управления АСУ РК (например, в части обработки данных, составляющих «пусковую ситуацию»);

- адаптировать внедряемые решения по защите от НСД/НСП к особенностям функциональных задач, решаемых в КШМ и СПУ (например, в части формирования единых порядка и правил информационного взаимодействия в рамках реализации соответствующих процедур управления).

Таким образом, применение в рамках технических средств КШМ и СПУ единых программно-аппаратных решений защиты от НСД/НСП, помимо соблюдения требования идеологической целостности реализуемой стратегии защиты, позволит уни-

фицировать состав используемых средств и, соответственно, улучшить их эксплуатационные характеристики. Как видно из рис. 3, система защиты от НСД/НСП СПУ структурно охватывает все уровни взаимодействия основных подсистем СПУ и соответствующих средств их управления (где ВКУП рассматривается как выносной терминал АРМа с ограниченным набором функций). Подобное структурное размещение системы защиты характерно и для КШМ с соответствующими поправками в части состава ее основных подсистем. Это позволяет, с одной стороны, осуществлять мониторинг состояния функциональных связей тракта боевого управления и проводить анализ заданного перечня текущих информационных процессов.

С другой стороны, такое размещение элементов системы защиты от НСД/НСП позволяет осуществлять блокирование и перехват функций управления при наступлении условий, классифицируемых ей, как факт совершения НСД/НСП.

В контексте вышесказанного необходимо подчеркнуть важность реализации в КБУ функций, связанных с документированием заданного перечня параметров информационного взаимодействия контролируемых подсистем при проведении пусков ракет и реализации некоторых важных процедур управления. При этом с точки зрения проецирования юридической ответственности на реализованные номерами боевых расчетов решения и действия, данный функционал систем защиты от НСД/НСП имеет безусловную важность.

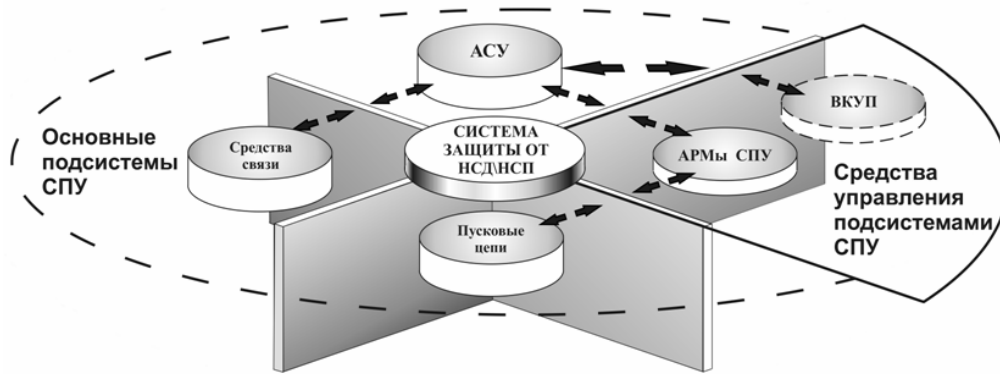


Рис. 3. Упрощенная схема взаимодействия системы защиты от НСД/НСП с основными функциональными подсистемами СПУ

Учитывая закрытый статус системы, исключая возможность «внешнего» вмешательства в ее целевой функционал, вся фиксируемая в ней информация является достаточным документальным основанием для формирования однозначных трактовок в случаях возникновения ситуаций, подпадающих под юрисдикцию вопросов НСД/НСП. В общем случае, использование в рамках систем защиты от НСД/НСП процедур регистрации информации обеспечивает «прозрачность» хода восстановления процессов формирования и выполнения заданного перечня задач управления, а также устраняет возможность обезличивания персональной ответственности должностных лиц, занятых в реализации циклов боевого управления.

Подводя итог рассмотрения проблематики защиты от НСД/НСП, можно сформулировать основные общесистемные принципы, которые, с нашей точки зрения, в наибольшей степени отражают внутреннюю суть рассмотренных процессов:

- комплексность защиты (применение организационных, технических и организационно-технических методов);
- многоуровневость (каскадирование) защитного функционала;
- непрерывность и автономность функционирования технической компоненты системы защиты;
- ключевая роль системы защиты при обеспечении контроля процессов информационного взаимодействия основных подсистем защищаемых объектов;
- унификация используемых программно-аппаратных решений системы защиты;
- вариативность логики функционирования, т.е. адаптация к типу и модификации защищаемых объектов;
- строгое ограничение доступа к обслуживанию элементов системы защиты;
- необходимость привлечения возможностей специально уполномоченной службы;
- предоставление полномочий на реализацию решений по применению оружия строго ограниченному (заданному) кругу должностных лиц;

– исключение возможностей обезличивания ответственности должностных лиц и обслуживающего персонала за принятые ими решения по применению оружия, управлению войсками и эксплуатации РК на всем протяжении его жизненного цикла.

Таким образом, разработка и внедрение унифицированного программно-аппаратного решения системы защиты от НСД/НСП, парирующей спектр актуальных угроз, в наибольшей степени соответствует современным взглядам военной науки в отношении путей развития РК СВ, а также особенностям организации их эксплуатации и боевого применения. Более того, с учетом обозначившейся устойчивой тенденции, связанной с постепенным усложнением вновь создаваемых систем оружия, использование в составе типового оснащения РК СВ унифицированных программно-аппаратных комплексов предотвращения НСД/НСП обеспечивает принципиально новую идеологию в реализации процедур легитимизации применения РК по назначению. При этом главная цель внедрения в войсковую практику подобных систем – это недопущение несанкционированного применения РК и предотвращение обезличивания ответственности должностных лиц ракетных формирований за принятые ими решения, связанные с применением оружия в любых условиях обстановки.

Выводы

1. В общем случае, решение вопросов защиты от НСД/НСП в РК СВ сводится к обеспечению требуемого уровня безопасности боевого управления и применения РК СВ в любых условиях оперативной и военно-политической обстановки.

2. С технической точки зрения реализация мероприятий по защите от НСД/НСП в РК СВ имеет своей главной целью комплексное обеспечение функций гарантированного предотвращения любых возможностей по осуществлению несанкционированных пусков ракет и несанкционированного делегирования полномочий.

3. С юридической точки зрения проведение мероприятий по защите от НСД/НСП находится в

плоскости обеспечения гарантий на реализацию решений по применению оружия и управление войсками строго заданному кругу лиц, с одной стороны, и четкой регламентацией фактической ответственности за принятые решения, с другой стороны.

4. Решение задачи создания унифицированной для различных типов РК СВ системы защиты от НСД/НСП носит комплексный характер и осуществляется путем реализации многоуровневой защиты, включающей в себя организационную, техническую, и в отдельных случаях криптографическую составляющие.

5. Специфика вопросов защиты от НСД/НСП обуславливает необходимость их безусловного распространения на весь жизненный цикл РК.

6. Необходимость целостного решения вопросов защиты от НСД/НСП требует от разработчиков новых образцов техники уже на этапе ее проектирования проводить оценку полноты выполнения соответствующих мероприятий. Использование такого подхода позволит обеспечить системность решения задачи защиты, что является основным залогом надежной и безопасной эксплуатации РК СВ впоследствии.

7. Процессы развития технологий и совершенствования форм и способов вооруженной борьбы обуславливают появление новых видов угроз, что требует постоянной корректировки круга задач, входящих в сферу ответственности системы защиты от НСД/НСП.

8. Состав, содержание и порядок выполнения мероприятий по предотвращению НСД/НСП являются вариативными составляющими защитного функционала системы защиты, сложность реализации которого пропорциональна количественному и качественному составу парируемых угроз.

9. Последствия, возникающие в результате несанкционированных действий или несанкционированных пусков, вне зависимости от причины их породившей, в одинаковой степени недопустимы и требуют обеспечения паритетной защиты для всего комплекса актуальных угроз.

10. Основными объектами инфраструктуры РК СВ, требующими внедрения рассмотренных решений защиты, являются КШМ и СПУ.

11. Рассмотренные особенности и основные общесистемные принципы санкционирования применения оружия РК СВ и выполнения особо важных процедур управления войсками (ракетными формированиями), при соответствующей их адаптации, могут быть распространены и на другие образцы систем вооружения, требующих по той или иной причине особого контроля за порядком их использования и применения по назначению.

Список литературы

1. Мухин В. Системные проблемы внедрения ЕСУ ТЗ [Электрон. ресурс]. – Режим доступа к ресурсу: http://nvo.ng.ru/armament/2011-10-14/1_esy_tz.html.
2. ОТРК "Искандер" (SS-26) – Электрон. ресурс. – Режим доступа к ресурсу: <http://topwar.ru/1914-otr-iskander-ss-26.html>.
3. Основы теории систем управления высокоточных ракетных комплексов Сухопутных войск / Б.Г. Гурский, М.А. Люцанов, Э.П. Спирин; под ред. В.Л. Солунина. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2001. – 328 с.
4. Димидюк Н. Автоматизация управления ракетной бригадой, вооруженной комплексом Р-17Э / Н. Димидюк, В. Иванов // Военный парад. – 2005. – 2(68). – С. 30-33.
5. Трансцендентная реализация централизованного управления телекоммуникационной сетью перспективного ракетного комплекса на основе принципов WMN-технологии / С.В. Малахов, А.Г. Снисаренко, С.Г. Рассомахин, Н.Ф. Линник, В.Н. Шлокин // Системы обработки информации. – Х.: ХУПС. – 2007. – Вып. 5(63). – С. 66-72.
6. Особенности обеспечения процедур обработки и обмена информацией в интегрированной системе автоматизированного управления и связи ракетных комплексов Сухопутных войск / М.М. Чеченков, С.В. Малахов, А.Г. Снисаренко, В.Н. Шлокин, А.Л. Гостев // Системы озброєння і військова техніка. – Х.: ХУПС. – 2010. – Вып. 4(24). – С. 80-87.
7. Стратегічний оборонний бюлетень України на період до 2015 року: (Біла книга України). – К.: Аванпост-прім, 2004. – 96 с.

Поступила в редколлегию 23.05.2012

Рецензент: д-р техн. наук, проф. В.В. Баранник, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ЗАГАЛЬНОСИСТЕМНІ ПИТАННЯ САНКЦІОНУВАННЯ ЗАСТОСУВАННЯ РАКЕТНИХ КОМПЛЕКСІВ СУХОПУТНИХ ВІЙСЬК

В.М. Шлокін, С.В. Малахов, О.Л. Гостєв, А.Г. Снісаренко, С.Г. Вдовенко, О.М. Присяжний

Розглянути загальні положення проблематики санкціонування застосування ракетних комплексів Сухопутних військ.

Ключові слова: ракетний комплекс, загрози, несанкціоновані дії, передача повноважень, сумісні дії.

GENERALSYSTEM QUESTIONS OF AUTHORIZATION OF ROCKET COMPLEXES OF OVERLAND ARMIES APPLICATION

V.N. Shlokin, S.V. Malakhov, A.G. Snisarenko, A.L. Gostev, S.G. Vdovenko, A.M. Prisyagniy

The general provisions of a problematics of authorization of application of rocket complexes of Overland armies are considered.

Keywords: a rocket complex, threats, non-authorized actions, transfer of powers, joint action.