УДК 621.391.05

А.Г. Снісаренко[1], С.В. Малахов[2], А.В. Щуцький[1]

[1] *Харківський університет Повітряних Сил імені Івана Кожедуба, Харків*
[2] *Харківський національний університет імені В.Н. Каразіна, Харків*

АКТУАЛЬНІ ПИТАННЯ БЕЗПЕКИ ЗАСТОСУВАННЯ ВИСОКОТОЧНИХ РАКЕТНИХ КОМПЛЕКСІВ

В статті розглянуті загальні положення проблематики безпечного застосування високоточних ракетних комплексів.

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

Вступ

Постановка проблеми. В процесі застосування нових зразків високоточних ракетних комплексів (ВРК) особливо гостро ставиться питання щодо необхідності забезпечення необхідного рівня безпеки їх застосування. В даному випадку під терміном „безпека застосування" ВРК будемо розуміти їх застосування за призначенням в суворій відповідності з керівними документами і, відповідно, з санкцією (дозволом) уповноваженої на це посадової особи.

При цьому, необхідно також враховувати і те, що однією із найважливіших систем сучасного високоточного РК є його автоматизована система управління (АСУ), яка, виступаючи сполучною ланкою між обслуговуючим персоналом і зброєю, своїми технічними характеристиками значною мірою визначає необхідний рівень контролю процедур управління і безпеки застосування ВРК [1, 6].

Аналіз останніх досліджень і публікацій. Рівень контролю процедур ініціалізації, видачі і виконання особливо важливих команд бойового управління і пускових циклограм ракетного комплексу (РК) як комплексний критерій, що враховує ступінь складності ухвалених технічних рішень та реалізації процедур обслуговування і бойового застосування РК, розглянуто в [1].

Якісні зміни в техніці, що відбуваються при створенні нових зразків і систем ВРК, та їх вплив на питання безпечного застосування розглянуті в [2 – 6].

Мета статті. Розглянуті як загальні положення щодо забезпечення безпеки застосування ВРК, так і специфічні питання передачі повноважень на прийняття рішення на застосування ракетної зброї посадовими особами різних ланок управління.

Виклад основного матеріалу

Розгляд зазначеної проблематики диктує необхідність проведення відповідного аналізу загроз безпечного застосування ВРК, які обумовлюються виникненням передумов здійснення несанкціонований дій (НСД) та несанкціонованих пусків ракет (НСП) в різних умовах експлуатації і застосування ВРК. При розгляді поняття НСД, мається на увазі те, що ці дії навмисно або ні можуть здійснювати особи бойової обслуги ланок управління які вже допущені до своїх робочих місць з певним рівнем повноважень щодо застосування ракетної зброї. Визначимо поняття НСД і НСП. Під несанкціонованими діями персоналу при експлуатації і бойовому застосуванні ВРК розумітимемо дії, що полягають в реалізації випадкової або умисної інформаційно-технічної дії на апаратуру АСУ ВРК і пускові ланцюги самохідних пускових установок (СПУ), які здатні привести:

– до зміни заданого (поточного) технічного стану і складу відповідних програмно-апаратних засобів ланок управління;

– до зміни ступеню бойової готовності ракетних формувань;

– до переприцілювання ракет, в т.ч. до зміни значень уставок цілевказівок;

– до зміни рангу підпорядкованості командних пунктів і/або поточних повноважень посадових осіб.

Під несанкціонованим пуском ракет за відсутності відповідних на це санкцій, що отримуються, як правило, із вищих (старших) щодо рангу підпорядкованості ланок управління (В(С)ЛУ), розумітимемо:

– несанкціонований запуск двигунної установки ракети;

– несанкціонований запуск пристрою міномет-ного старту;

– пуск ракети по незапланованій цілі;

– пуск ракети без введеного польотного завдання.

За наслідками аналізу специфіки умов експлуатації і особливостей бойового застосуванні ВРК можна сформувати наступні дві групи загроз виникнення передумов здійснення НСД/НСП:

– загрози організаційного характеру;

– загрози технічного характеру.

До групи загроз організаційного характеру доцільно віднести такі:

– неодноразові порушення заданого порядку реалізації сумісних дій номерами бойової обслуги ланки управління;

– неодноразові спроби підбору пароля, що надає право роботи на відповідній апаратурі ланки управління;

– неправомірна передача повноважень (права бойової роботи на апаратурі ланки управління) між номерами бойової обслуги ланки управління;

– навмисні або ненавмисні дії, що полягають в спробах зміни заданих зі СЛУ режимів функціонування апаратури даної ланки управління;

– навмисні або ненавмисні дії, що полягають в спробах нелегітимної передачі органам управління нижчої ланки управління повноважень по формуванню ними пускових команд/наказів або управлінню елементами інших ланок управління;

– виконання дій під примусом;

– несанкціонований зі СЛУ набір і введення в систему управління заданого переліку особливо важливих наказів/команд, що складають пускову ситуацію;

– неавторизована зміна складу апаратури і програмних засобів системи управління командно-штабних машин (КШМ) і СПУ, а також пускових ланцюгів СПУ;

– спроби неправомірного відключення, демонтажу або порушення цілісності елементів системи захисту від НСД/НСП;

– видача в канали зв'язку контрольної інформації при проведенні технічного обслуговування апаратури ланки управління.

До групи загроз технічного характеру доцільно віднести наступні:

– виникнення програмно-апаратних збоїв в роботі апаратури АСУ і зв'язку та спеціальних блокуючих пристроїв (СБП) КШМ і СПУ, а також пускових ланцюгів СПУ;

– порушення функціонування апаратури АСУ і зв'язку внаслідок їх придушення і/або нав'язування хибної інформації або порушень режимів електроживлення.

Нейтралізація приведених вище загроз забезпечує найбільш адекватний, з погляду нейтралізації їх наслідків, ефект. З погляду нейтралізації загроз, використання вищенаведеного порядку їх групування дозволяє проявити найбільш критичні особливості, характерні для різних умов застосування ВРК, і створює достатню основу для формування пропозицій щодо складу і змісту заходів, направлених на запобігання наслідкам цих загроз.

Разом з вищесказаним необхідно відзначити той факт, що питання реалізації заходів щодо захисту від НСД/НСП де-факто мають свої технічну і юридичну сторони. Так, з технічної точки зору, виконання заходів щодо захисту від НСД/НСП мають своєю метою комплексне забезпечення функцій блокування будь-яких можливостей щодо здійсненню несанкціонованих пусків ракет і реалізації заданого переліку особливо важливих процедур управління зброєю і військами. Юридична ж сторона питання знаходиться в площині забезпечення гарантій на реалізацію рішень по застосуванню зброї суворо заданому колу осіб, з одного боку, і чіткою регламентацією фактичної відповідальності за ухвалені ними рішення на застосування зброї і управління військами, з іншого боку.

Оскільки в ієрархічних системах управління сучасних РК Сухопутних військ [3, 4] на різних етапах їх циклів бойового управління задіяні як технічні засоби, так і обслуговуючий персонал (номери бойових обслуг), то очевидно, що в якості джерел виникнення НСД/НСП необхідно розглядати як дії номерів бойових обслуг (людський або організаційний чинник виникнення НСД/НСП), так і безпосередньо самі технічні засоби системи управління РК і пускових ланцюгів СПУ (технічний чинник виникнення НСД/НСП).

На нашу думку, в перспективних ВРК комплексні системи захисту від НСД/НСП по складу вирішуваних ними завдань і специфіці інтеграції спеціальних пристроїв до складу устаткування різних елементів РК, ідентичні як для РК із звичайним, так і з високоточним оснащенням. При цьому, для високоточних РК основні відмінності в реалізації подібних систем полягають в розширенні переліку постійно контрольованих параметрів основних систем РК, що реалізується шляхом зміни конфігурації спеціального програмного забезпечення (СПО) системи захисту від НСД/НСП, а також розширенням якісного і кількісного складу датчиків і виконавчих елементів системи захисту.

Подібна схожість систем захисту, що реалізовуються в РК із звичайним і високоточним оснащенням, обумовлена вкрай вузькою цільовою спрямованістю подібних систем захисту, у будь-якому випадку вирішуючих два основні завдання:

1. Санкціонування застосування зброї, тобто легітимізація проведення пусків ракет.

2. Захист від несанкціонованих дій обслуговуючого персоналу РК при реалізації особливо важливих процедур управління (наприклад, при передачі органами управління верхніх ланок частини своїх повноважень нижнім ланкам по управлінню ракетними формуваннями та ракетною зброєю).

Таким чином, рішення задачі формування вимог до функцій і складу завдань системи захисту від НСД/НСП повинне спиратися на результати аналізу і систематизації загроз, характерних для конкретних типів РК. В результаті цього створюються необхідні умови для розроблення адекватної стратегії захисту, уточнення її основних принципів, і, як наслідок, визначення необхідного складу і комбінації відповідних методів і способів парирування всієї сукупності актуальних загроз.

У загальному випадку, стосовно специфіки ВРК можна виділити три основні групи методів захисту: організаційні; алгоритмічні; програмно-технічні.

Як приклад основних організаційних методів можна привести наступні:

– суворе виконання заходів щодо технічного захисту інформації (розмежовування доступу до інформації управління);

– організація чергування з метою виключення випадкового або навмисного доступу не уповноважених осіб до апаратури ланок управління;

– виконання особливо важливих операцій бойового управління з використанням номерами бойових обслуг алгоритму сумісних дій;

– реалізація в циклах управління системи періодичних доповідей про стан і боєготовність ланок управління і ін.

Алгоритмічні методи базуються на ідеології системного захисту від спроб формування і введення в систему управління РК несанкціонованих наказів і команд управління, включаючи несанкціонований доступ до інформації бойового управління. Основою алгоритмічного захисту є концепція використання спеціального блокуючого пристрою, що грає головну роль в реалізації функцій захисту трактів бойового управління КШМ і СПУ, а також пускових ланцюгів СПУ при проходженні по ним пускових наказів і інших особливо важливих команд управління (наприклад, на перевід ланки управління з одного ступеня готовності в іншу). Крім того, до групи алгоритмічних методів запобігання НСД/НСП слід віднести і практику використання методу накопичення «пускової ситуації». Відповідно до нього здійснення пусків будь-якою з ланок управління можливо тільки при виконанні заданого переліку обов'язкових логічних умов, пов'язаних з аналізом поточного стану інформаційних процесів і параметрів системи управління РК, детальний розгляд яких, виходить за рамки даної публікації. Програмно-технічні методи захисту від НСД/НСП передбачають використання засобів, що дозволяють запобігти можливим негативним наслідкам, які виникають унаслідок проведення випадкових або навмисних (в т.ч. нештатних або помилкових) дій обслуговуючого персоналу. До основних з них слід віднести:

– використання номерами бойових обслуг КШМ і СПУ атрибутів розмежування доступу до здійснення функцій бойового управління;

– впровадження практики використання змінних паролів на період виконання конкретних бойових завдань;

– автоматичне документування дій номерів бойових обслуг;

– реалізація номерами бойових обслуг КШМ і СПУ алгоритму сумісних дій при введенні в систему управління інформації, що відноситься до категорії особливо важливих процедур управління, зокрема при проведенні пусків ракет.

Підводячи підсумок розгляду проблематики захисту від НСД/НСП, сформулюємо основні принципи, які, на наш погляд, найбільшою мірою відображають внутрішню суть розглянутих процесів:

– комплексність захисту (застосування організаційних, технічних і організаційно-технічних методів);

– багаторівневість (каскадування) захисного функціоналу;

– безперервність і автономність функціонування технічної компоненти системи захисту;

– ключова роль системи захисту при забезпеченні контролю процесів інформаційної взаємодії основних підсистем об'єктів, що захищаються;

– уніфікація використовуваних програмно-апаратних рішень системи захисту;

– вариативність логіки функціонування, тобто адаптація до типу і модифікації об'єктів, що захищаються;

– суворе обмеження доступу до обслуговування елементів системи захисту;

– надання повноважень на реалізацію рішень по застосуванню зброї суворо обмеженому (заданому) колу посадових осіб;

– виключення можливостей знеособлення відповідальності посадових осіб і обслуговуючого персоналу за ухвалені ними рішення щодо застосування зброї, управлінню військами і експлуатації ВРК на всьому протязі його життєвого циклу.

Таким чином, розробка і впровадження уніфікованого програмно-апаратного рішення системи захисту від НСД/НСП, що парирує спектр актуальних загроз, найбільшою мірою відповідає сучасним поглядам військової науки відносно шляхів розвитку ВРК, а також особливостям організації їх безпечної експлуатації і бойового застосування.

І, на закінчення, розглянемо особливості організації захисту від НСД при передачі повноважень.

В аспекті передачі повноважень щодо управління підлеглими ланками управління, включаючи і управління зброєю, необхідно розглядати два аспекти.

Перший аспект пов’язаний з передачею повноважень ВЛУ. Як правило, ця передача обумовлюється заздалегідь на одну із наявних СЛУ, доводиться до інших СЛУ і відображається у нормативному документі. Здійснення заздалегідь обумовленої передачі повноважень відбувається в разі виходу з ладу (знищення) ВЛУ. При цьому, СЛУ, яка взяла на себе функції ВЛУ з використанням спеціальних наказів/команд зі складу інформаційного забезпечення АСУ доводить про цей факт іншим ланкам управління. При формуванні та видачі таких наказів/команд повинен бути використаний алгоритм сумісних дій номерів бойової обслуги як дієвий елемент захисту від НСД.

Другий аспект передачі повноважень пов’язаний з випадковим (епізодичним) характером і реалізується, виходячи з оперативної обстановки, що складається.

Випадковий характер передачі повноважень стосується випадку, коли визначена заздалегідь СЛУ так же як і ВЛУ із поважних причин не може здійснювати функції щодо управління підлеглими ланками, а також у випадку, коли СЛУ і підпорядковані їй підрозділ (підрозділи) діють відокремлено від ВЛУ. В цьому випадку виникає необхідність встановлення повноважень СЛУ як ВЛУ. При цьому можливо задіяти наступний механізм встановлення повноважень:

ввід на ланці управління відповідного режиму функціонування апаратури АСУ; ввід спеціальних наказів/команд зі складу інформаційного забезпечення АСУ про факт встановлення повноважень ВЛУ іншим ланкам управління. При вводі відповідного режиму функціонування апаратури АСУ ланки управління та формуванні та видачі наказів/команд на взяття повноважень також повинен бути використаний алгоритм сумісних дій номерів бойової обслуги як дієвий елемент захисту від НСД.

Епізодичний характер передачі повноважень стосується тимчасового надання конкретній посадовій особі ланки управління повноважень на самостійне прийняття рішень щодо управління підлеглими їй ланками та застосування зброї залежно від обстановки, що складається, без окремої подальшої на це санкції із ВЛУ. Передача повноважень в цьому випадку може бути здійснена з використанням механізму „кінцевої" адресації наказів/команд. Суть данного механізму полягає в тому, що у випадку видачі відповідного(ої) наказу/команди на подальше самостійне управління підлеглими підрозділами чи зброєю в адресній частині формалізованої кодограми, що здійснює передачу цього наказу/команди, вказується адреса СЛУ без транзитного признаку передачі. Саме цей факт і є підтвердженням передачі повноважень щодо санкціонування подальших самостійних дій. Необхідно підкреслити, що при передачі повноважень щодо подальшого управління ракетною зброєю, СЛУ в разі отримання повноважень здійснює управління по видачі наказів/команд, що створюють пускову ситуацію і які раніше не видавались ВЛУ.

Таким чином, розглянутий порядок організації передачі повноважень між ланками управління в різних умовах застосування ВРК виступає простим але, разом з тим, дієвим засобом захисту від НСД/НСП.

Висновки

1. У загальному випадку, проблематика безпеки застосування ВРК, в значній мірі, зводиться до вирішення питань захисту від НСД/НСП.

2. З технічної точки зору реалізація заходів щодо захисту від НСД/НСП у ВРК має своєю головною метою комплексне забезпечення функцій гарантованого запобігання будь-яким можливостям по здійсненню несанкціонованих пусків ракет і несанкціонованого делегування повноважень.

3. З юридичної точки зору проведення заходів щодо захисту від НСД/НСП знаходиться в площині забезпечення гарантій на реалізацію рішень по застосуванню зброї і управлінні військами суворо заданому колу осіб, з одного боку, і чіткою регламентацією фактичної відповідальності за ухвалені рішення, з іншого боку.

4. Рішення задачі створення уніфікованої для різних типів РК системи захисту від НСД/НСП носить комплексний характер і здійснюється шляхом реалізації багаторівневого захисту, що включає організаційну і технічну складові.

5. Організація передачі повноважень між ланками управління повинна забезпечувати захист від НСД/НСП з урахуванням особливостей застосування ВРК.

6. Специфіка питань захисту від НСД/НСП обумовлює необхідність їх безумовного розповсюдження на весь життєвий цикл РК.

7. Склад, зміст і порядок виконання заходів щодо запобігання НСД/НСП є вариативными складовими захисного функціоналу системи захисту, складність реалізації якого пропорційна кількостному і якісному складу парируваних загроз.

Список літератури

1. Общесистемные вопросы санкционирования применения ракетных комплексов Сухопутных войск / В.Н. Шлокин, С.В. Малахов, А.Г. Снисаренко, А.Л Гостев, С.Г. Вдовенко, А.М. Присяжный // Системи озброєння і військова техніка. – Х.: ХУПС, 2012. – Вип. 2(30). – С. 78-87.

2. ОТРК "Искандер" (SS-26) [Електрон. ресурс]. – Режим доступу: http://topwar.ru/1914-otrk-iskander-ss-26.html.

3. Основи теорії систем управління високоточних ракетних комплексів Сухопутних військ / Б.Г. Гурський, М.А. Лющанов, Е.П. Спірін; під ред. В.Л. Солуніна. – М.: Вид-во МГТУ ім. Н.Е. Баумана, 2001. – 328.

4. Дімідюк Н. Автоматізация управління ракетною бригадою, озброєною комплексом Р-17е / Н. Дімідюк, В. Іванов // Військовий парад. – 2005. – 2(68). – С. 30-33.

5. Трансцендентна реалізація централізованого управління телекомунікаційною мережею перспективного ракетного комплексу на основі принципів WMN-технологии / С.В. Малахов, А.Г. Снісаренко, С.Г. Рассомахін, Н.Ф. Лінник, В.Н. Шлокін // Системи обробки інформації. – Х.: ХУПС, 2007. – Вип. 5(63). – С. 66-72.

6. Особливості забезпечення процедур обробки і обміну інформацією в інтегрованій системі автоматизованого управління і зв'язку ракетних комплексів Сухопутних військ / М.М. Чеченков, С.В. Малахов, А.Г. Снісаренко, В.Н. Шлокін, А.Л. Гостев // Системи озброєння і військова техніка. – Х.: ХУПС, 2010. – Вип. 4(24). – С. 80-87.

Надійшла до редколегії 22.12.2015

Рецензент: д-р техн. наук, проф. Ю.В. Стасєв, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

АКТУАЛЬНЫЕ ВОПРОСЫ БЕЗОПАСНОСТИ ПРИМЕНЕНИЯ ВЫСОКОТОЧНЫХ РАКЕТНЫХ КОМПЛЕКСОВ

А.Г. Снисаренко, С.В. Малахов, А.В. Щуцкий

Рассмотрены общие положения проблематики безопасного применения высокоточных ракетных комплексов.

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

THE TOPICAL QUESTIONS ARISES AS TO APPLICATION SAFETY OF HIGH-FIDELITY ROCKET COMPLEXES

A.G. Snisarenko, S.V. Malakhov, A.V. Syutsky

In the articles considered generals position of problematic of safe application of high-fidelity rocket complexes.

Keywords: *rocket complex, threats, unauthorized actions, delegation of powers.*