УДК: 004.056 DOI: 10.53816/23061456_2022_7–8_77

АНАЛИЗ ИНФОРМАЦИОННО-ТЕХНИЧЕСКОГО ВОЗДЕЙСТВИЯ НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

ANALYSIS OF INFORMATION TECHNOLOGY IMPACT ON SPECIAL PURPOSE INFORMATION SYSTEMS

О.П. Шеметов, И.В. Чечин, канд. техн. наук С.А. Диченко, д-р техн. наук Д.В. Самойленко

O.P. Shemetov, I.V. Chechin, Ph.D. S.A. Dichenko, D.Sc. D.V. Samoylenko

Краснодарское высшее военное училище им. С.М. Штеменко

Развитие информационных систем специального назначения способствовало их интеграции в концепцию сетецентрической войны, что и стало поводом их активного применения в Вооруженных Силах Российской Федерации. В концепции сетецентрической войны робототехнические комплексы, с точки зрения безопасности информации можно рассматривать как удаленные информационные системы. В условиях совершенствования средств информационно-технического воздействия на информационные системы возникают угрозы безопасности информации, циркулирующей в робототехнических комплексах. Проведен анализ информационно-технических воздействий на робототехнические комплексы специального назначения с целью выявления их уязвимостей, а также последствий деструктивных воздействий, связанных с применением средств радиоэлектронного подавления, характеризуемого нарушением целостности, доступности и конфиденциальности информации.

Ключевые слова: робототехнический комплекс военного назначения, информационно-техническое воздействие, информационная система, безопасность информации, радиоэлектронное подавление, компьютерная разведка.

The development of special-purpose information systems contributed to their integration into the concept of network-centric warfare, which became the reason for their active use in the Armed Forces of the Russian Federation. In the concept of network-centric warfare, robotic complexes, from the point of view of information security, can be considered as remote information systems. In the conditions of improving the means of information and technical impact on information systems, threats to the security of information circulating in robotic complexes arise. The analysis of information and technical impacts on special-purpose robotic complexes has been carried out in order to identify their vulnerabilities, as well as the consequences of destructive effects associated with the use of electronic suppression equipment characterized by a violation of the integrity, accessibility and confidentiality of information.

Keywords: military robotic complex, information technology impact, information system, information security, electronic countermeasures, computer intelligence.

Введение

Результаты анализа опыта военных конфликтов, имевших место на рубеже XX–XXI веков, показывают, что современные боевые действия, ведущиеся в соответствии с концепцией сетецентрической войны, характеризуются следующими основными особенностями: возрастание роли информационного противоборства, использование нетрадиционных форм ведения

боевых действий, повышение точности и избирательности действия оружия, внедрение новых систем управления, разведки, компьютерного моделирования. Исходя из этих особенностей общими технологическими тенденциями развития вооружения являются: интеллектуализация, миниатюризация, снижение энергопотребления, многофункциональность, автономность, снижение веса и удобство снабжения [1, 2].

В концептуально-теоретическом плане модель сетецентрической войны представляет собой систему, состоящую из двух основных подсистем (средств разведки и средств поражения), объединенных воедино органами управления и командования [3].

Сетецентрическое ведение боевых действий характеризуется не только обеспечением передачи развединформации всем участникам этих действий в реальном масштабе времени, но и высоким уровнем организации (самоорганизации) функционирования элементов боевого построения.

Робототехнические комплексы военного назначения (РТК ВН) могут эффективно использоваться в качестве элементов обеих подсистем системы сетецентрической войны. Поэтому уже при разработке роботизированных образцов вооружения и военной техники (ВВТ) необходимо прорабатывать вопросы их интеграции в единый контур управления войсками на различных уровнях (тактический, оперативный, стратегический).

РТК ВН могут являться как самостоятельным средством ведения боевых действий, так и (или) дополнять традиционные виды оружия во всех формах и способах боевых и специальных действий при решении различных задач (рис. 1), обеспечивая достижение поставленных целей при сокращении потерь личного состава и снижении человеческого фактора.

Следует отметить, что указанные задачи являются достаточно общими и при разработке конкретных роботизированных образцов ВВТ необходимо проведение исследований с целью уточнения их роли и места с учетом нового облика Вооруженных Сил Российской Федерации (ВС РФ) и их оргштатной структуры, оценки готовности научно-технологического задела, возможных способов и эффективности применения [4].

В соответствии со взглядами отечественных и зарубежных специалистов в боевых действиях будущего одними из наиболее перспективных видов системы управления, связи и безопасности ВВТ, интегрирующими большинство из перечисленных направлений, будут РТК ВН.

Одним из основных ограничений на применение РТК ВН является его необходимость постоянного взаимодействия с оператором. Таким образом, несмотря на десятки разрабатываемых систем автоматического управления, РТК ВН продолжают быть управляемыми человеком. Они нуждаются в человеческом контроле, иначе применять их будет попросту невозможно, что приводит к постоянному обмену информацией [1].

РТК ВН в традиционном понимании по ряду признаков и выполняемых функций (сбор, хранение, обработка и распространение информации) может быть интерпретирована как информационная система (ИС) обработки информации [5].

Как и любая ИС, РТК ВН содержит в своем составе совокупность средств вычислительной техники, что делает его целевым объектом для информационно-технического воздействия (ИТВ) со стороны противника. Под ИТВ будем понимать процесс непосредственного информационно-технического поражения/подавления информационно-технических объектов (целей) [6]. Исходя из этого, ИТВ направлено на нарушение устойчивого функционирования РТК ВН.

Под устойчивым функционированием РТК ВН как ИС, в общем виде, понимается такое состояние, при котором обеспечивается возможность выполнения (реализации) функций по обработке информации. Под обработкой информации будем понимать совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения информации.

Нарушение качественных характеристик информации, определяющих ее пригодность в решении целевых функций РТК ВН, может нанести неприемлемый ущерб субъектам информационного взаимодействия. В условиях ИТВ при решении критически значимых задач вероятность получения ущерба значительно увеличивается [5].

Уязвимости РТК ВН

В ходе активного применения РТК ВН в военных конфликтах были выявлены уязвимости информационной безопасности (ИБ). Случаи реализации ИТВ на РТК ВН представлены ниже.

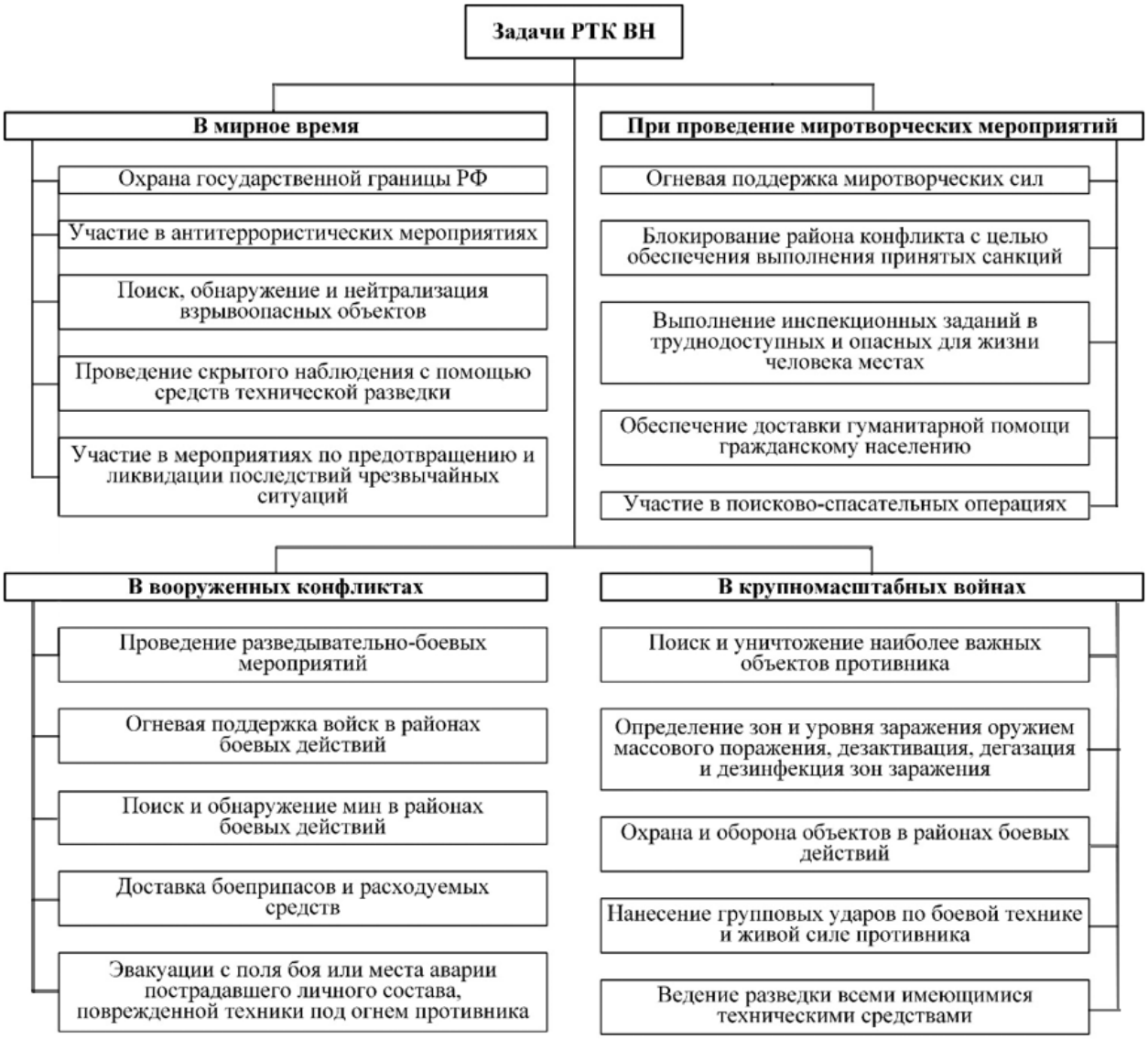

Рис. 1. Задачи РТК ВН

4 декабря 2012 года мировые СМИ, ссылаясь на информацию иранских источников, сообщили, что средства радиоэлектронной борьбы Ирана посадили на востоке страны американский беспилотник RQ-170 «Sentinel». 8 декабря Иран обнародовал короткую видеозапись, из которой ясно, что аппарат находится в руках иранских военных. На видеоматериале видно, что он не получил практически никаких внешних повреждений. Были обнародованы и некоторые параметры аппарата. В данном случае иранскими специалистами была использована уязвимость, связанная с тем, что в управлении беспилотными летательными аппаратами есть слабое звено — необходимость постоянного обмена информацией с наземными пунктами управления, а также использование внешней системы позиционирования в пространстве.

В октябре 2011 года атаке подверглась система базы США Крич в штате Невада, сообщает со ссылкой на собственные источники американский журнал Wired. Именно с этой базы управляют беспилотниками типа «Predator» и «Reaper», которые участвуют в военных действиях во многих странах мира, в том числе в Ираке и Афганистане. США отказались от комментариев, лишь отметив: «Мы вообще не обсуждаем деталей уязвимостей, угроз, или атак на наши компьютерные сети, так как это облегчает задачу злоумышленникам».

Летом 2009 года американские войска обнаружили на ноутбуках иракских повстанцев программное обеспечение, позволяющее перехватывать видео с беспилотников, которое передавалось в командные пункты по незашифрованным каналам связи. Некоторые информационные источники заявили, что повстанцы воспользовались программным продуктом малоизвестной российской фирмы стоимостью 25 долларов. По данным американских военных, такая практика установилась в Ираке с середины 2008 года. Это стало возможно из-за того, что на БПЛА RQ/MQ-1 «Predator» и MQ-9 «Reaper» используются нешифрованные каналы связи [7].

Исходя из вышеуказанных случаев можно определить уязвимости БИ:

– необходимость постоянного обмена информацией с пунктами управления (ПУ);

– использование незащищенных криптографическими методами каналов связи.

ИТВ, направленное на РТК ВН средствами радиоэлектронного подавления

Каналы обмена информацией с ПУ необходимы для постоянного контроля и управления РТК ВН. По ним передаются данные различного типа, уровня важности, объема, уровня криптозащиты и т.д. Для обмена данными организуются следующие каналы связи:

– канал связи для передачи команд управления, а также команд управления специальной аппаратурой и техническими средствами полезной нагрузки, размещенными на РТК ВН;

– канал связи для передачи телеметрической информации о состоянии подсистем РТК ВН, специальной аппаратуры и технически средств полезной нагрузки, а также квитанций о выполнении команд управления и высокоскоростной передачи данных от специальной аппаратуры и технических средств специальной нагрузки, размещенной на РТК ВН.

Перспективным направление ИТВ является применение средств радиоэлектронного подавления (РЭП), способы применения, основные преимущества и недостатки которых представлены на рис. 2.

Для подавления каналов передачи данных и управления РТВ ВН применяются следующие типы помех:

– помехи, перекрывающие рабочий диапазон частот (белый шум высокой мощности, одночастотное или модулированное гармоническое колебание);

– помехи, прицельные по частоте линий управления и связи (шумовая помеха, гармоническая помеха, имитирующая помеха) [4].

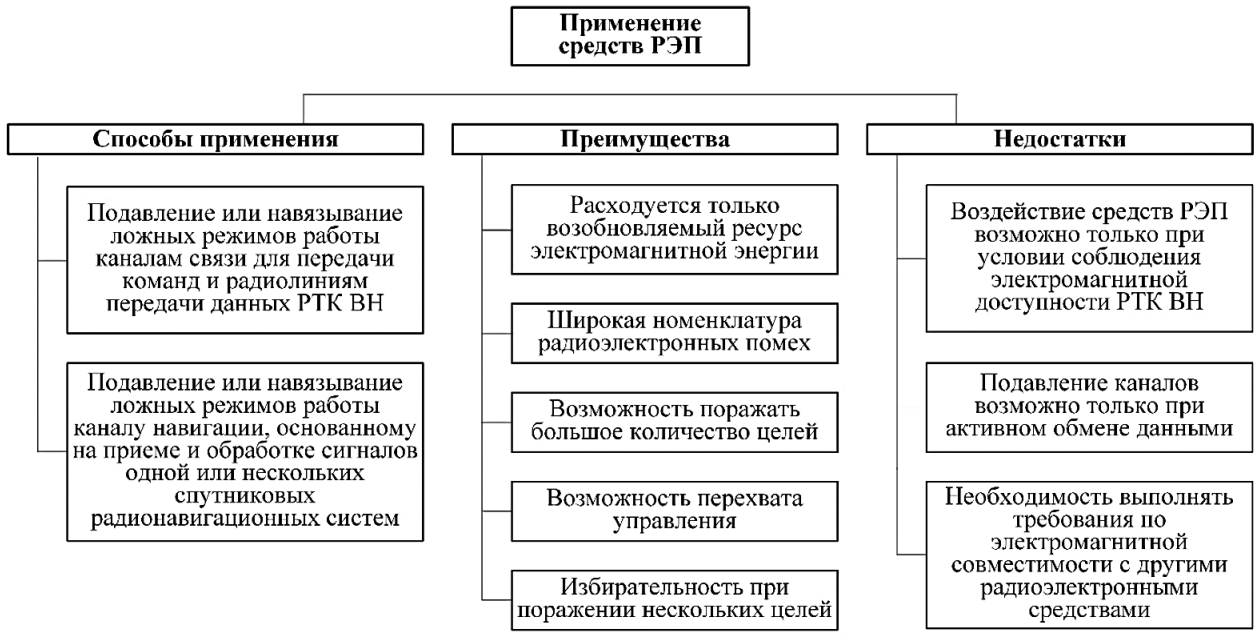

Рис. 2. Обобщенная характеристика средств РЭП

Средства РЭП являются высокоэффективным и перспективным средством противодействия РТК ВН. Особо подвержен деструктивному воздействию высокоскоростной канал передачи данных от РТК ВН на пункт управления. В силу передачи по нему большого объема информации, требует большой полосы частот, что способствует успешной реализации ИТВ средствами РЭП. Деструктивное воздействие приводит к нарушению взаимодействия между ПУ и РТК ВН, но не может гарантировать полное прекращение функционирования РТК ВН, в силу предусмотренных режимов работы в условиях радиоэлектронного подавления. При этом вышеуказанные недостатки (рис. 2) накладывают ограничения на успешное применение средств РЭП.

ИТВ, направленные на РТК ВН как на ИС

В условиях сетецентрической войны, где все средства разведки и средства поражения объединяются в единую распределенную ИС, позволяет рассматривать РТК ВН как составную часть данной системы. При рассмотрении РТК ВН как ИС, передаваемые по каналам связи данные несут не только сведения, полученные/переданные РТК ВН, в ходе выполнения своих функций, но и техническую информацию о структуре и порядке взаимодействия составных частей распределенной ИС. Для анализа технической информации применяют средства форматной, потоковой и сетевой компьютерной разведки. Целями компьютерной разведки (КР) является вскрытие формата и протокола передаваемых по каналам связи. Реализация ИТВ средствами КР на каналы связи возможна при использовании средств криптографической защиты информации (СКЗИ) с низкой криптоустойчивостью, или СКЗИ не используется вообще.

С получением доступа средств КР к передаваемым данным появляется возможность провести анализ формата, структуры и особенностей информации, циркулирующей между ПУ и РТК ВН. Результаты анализа представлены на рис. 3.

Вышеуказанные данные могут характеризовать РТК ВН как стандартную удаленную ИС с доступом к ней через канал радиосвязи [4].

При рассмотрении РТК ВН как ИС могут быть реализованы следующие виды ИТВ:

– направленные на нарушение доступности РТК ВН или ПУ;

– направленные на нарушение конфиденциальности и целостности связи между РТК ВН и ПУ;

– направленные на нарушение целостности и доступности операционной системы (ОС) или программного обеспечения (ПО) на РТК ВН или ПУ.

ИТВ, направленные на нарушение доступности РТК ВН или ПУ

К данному виду ИТВ можно отнести удаленные атаки типа «отказ в обслуживании». Атака «отказ в обслуживании» направлена на блокировку доступа к объекту путем исчерпания его ресурсов за счет отправки большого числа запросов к нему.

Типы удаленных атак представлены на рис. 4.

Атака «отказ в обслуживании» классифицируется как активное воздействие, осуществляемое с целью нарушения работоспособности системы, безусловная относительно цели атаки.

Рис. 3. Результаты анализа данных с помощью средств КР

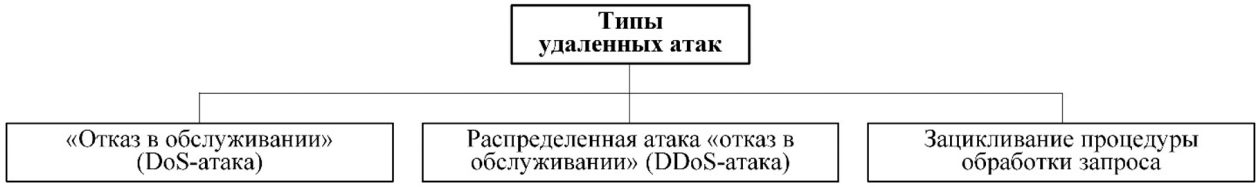

Рис. 4. Типы атак «отказ в обслуживании»

Данная атака является однонаправленным воздействием, осуществляемым как межсетевым, так и внутрисетевым образом, осуществляемым на сетевом, транспортном и прикладном уровнях модели OSI [8, 9].

Последствиями такого воздействия является нарушение ИБ, выражавшееся в прекращения штатного функционирования РТК ВН, из-за перегрузки аппаратной части.

ИТВ, направленные на нарушение конфиденциальности и целостности связи между РТК ВН и ПУ

К данному виду ИТВ относится внедрение ложного объекта в ИС. Внедряемым ложным объектом может быть как ложный ПУ, так и «виртуальный» РТК ВН. Зачастую в распределенной ИС бывают недостаточно надежно решены проблемы идентификации сетевых управляющих устройств при их взаимодействии с объектами системы. В этом случае такая система может подвергнуться сетевой атаке, связанной с изменением параметров маршрутизации и внедрением в сеть ложного объекта. В том случае, если настройки сети таковы, что для взаимодействия объектов необходимо использовать алгоритмы удаленного поиска узлов, то это также может быть использовано для внедрения в систему ложного объекта.

Таким образом, существуют два способа проведения атаки «внедрение ложного объекта в ИС»:

– внедрение ложного объекта путем навязывания ложного сетевого маршрута;

– внедрение ложного объекта путем использования недостатков алгоритмов адресации и удаленного поиска узлов в сети.

В случае использования в ИС механизмов удаленного поиска существует возможность на атакующем объекте перехватить посланный запрос и послать на него ложный ответ, где указать данные, использование которых приведет к адресации на атакующий ложный узел. В дальнейшем весь поток информации между субъектом и объектом взаимодействия будет проходить через этот ложный объект ИС.

Другой вариант внедрения в ИС ложного объекта использует недостатки алгоритма удаленного сетевого поиска и состоит в периодической передаче на атакуемый объект заранее подготовленного ложного ответа без приема поискового запроса. Такая удаленная атака чрезвычайно распространена в глобальных сетях, когда у атакующего, из-за нахождения его в другом сетевом сегменте относительно цели атаки, просто нет возможности перехватить поисковый запрос [9].

Целями внедрения ложного ПУ является перехват управления РТК ВН и навязывание ложных команд, а ложного РТК ВН, который передает ПУ ложную телеметрическую информацию, ввести ПУ в заблуждение [4].

ИТВ, направленные на нарушение целостности и доступности ОС или ПО на РТК ВН или ПУ

К данному виду ИТВ относят компьютерные вирусы и программно-аппаратные закладки.

Компьютерные вирусы в соответствии со способами распространения и вредоносной нагрузкой можно классифицировать по четырем основным типам: классические вирусы, программы типа «червь», программы типа «троян», другие вредоносные программы.

Основное свойство классического компьютерного вируса — это способность к саморазмножению. Путями проникновения вируса могут служить мобильные носители, сетевые соединения, а также любые другие каналы, по которым можно скопировать файл. Однако в отличие от «червей», вирусы не используют сетевые ресурсы — заражение вирусом возможно, только если

пользователь сам каким-либо образом его активировал. Основная цель вируса — распространение на другие ИС и выполнение деструктивных действий при определенных событиях или действиях пользователя.

В отличие от классических вирусов программы типа «червь» — это вполне самостоятельные программы, которые также способны к саморазмножению, однако при этом они способны и к самостоятельному распространению с использованием сетевых каналов. Для подчеркивания этого свойства иногда используют термин «сетевой червь». Программа типа «червь» — это программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению подсистем защиты ИС, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом.

В отличие от вирусов и червей в программах типа «троянский конь» не всегда предусмотрен функционал саморазмножения. Довольно большая часть таких программ функцией саморазмножения вообще не обладает. Программа типа «троян» («троянский конь») — программа, основной целью которой является вредоносное воздействие по отношению к ИС путем выполнения несанкционированных действий, а именно кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности ИС или несанкционированное использования ее ресурсов. Некоторые «трояны» способны к самостоятельному преодолению подсистемы защиты ИС, с целью проникновения в нее. Однако в большинстве случаев они проникают в систему вместе с вирусом либо с червем. В этом случае вирус или червь следует рассматривать как средство доставки, а «троян» — как средство информационного поражении.

Программной закладкой является скрытно внедренная в защищенную ИС программа либо намеренно измененный фрагмент программы, которая позволяет осуществить несанкционированный доступ к ресурсам системы на основе изменения свойств системы защиты.

Программные закладки, получая несанкционированный доступ к данным в памяти ИС, перехватывают их. После перехвата эти данные копируются и сохраняются в специально созданных разделах памяти или передаются по сети. Программные закладки, подобно вирусам, могут искажать или уничтожать данные, но в отличие от вирусов деструктивное действие таких программ, как правило, более выборочно и направлено на конкретные данные.

Аппаратной закладкой является устройство в электронной схеме, скрытно внедряемое к остальным элементам, которое способно вмешаться в работу аппаратных средств ИС. Результатом работы аппаратной закладки может быть как полное выведение системы из строя, так и нарушение ее нормального функционирования, например несанкционированный доступ к информации, ее изменение или блокирование [9].

Внедрение в управляющие ОС или ПО компьютерных вирусов или внедрение в РТК ВН программно-аппаратных закладок влечет за собой нарушение функционирования ОС или ПО, а также перехват управления РТК ВН [4].

Вывод

Таким образом, определены уязвимости ИБ в РТК ВН в условиях современного ИТВ. Проведен анализ перспективных средств ИВТ, в ходе которого было определено, что применение ИТВ на основе только средств РЭП не эффективно. Успешная реализация ИТВ на РТК ВН возможна при комплексном применении вышеуказанных средств и способов.

Результаты, полученные при анализе ИТВ и уязвимостей РТК ВН, позволяют определить актуальные направления в области защиты информации в условиях постоянного ИТВ направленного на РТК ВН, а также сделать вывод о требуемых в настоящее время механизмах развития приоритетных направлений повышения эффективности системы вооружения, обеспечивающей гарантированное управления войсками (силами) и оружием в условиях внедрения перспективных информационных технологий при создании и использовании ИС специального назначения.

Литература

1. Макаренко С.И. Робототехнические комплексы военного назначения — современное состояние и перспективы развития // Системы управления, связи и безопасности. 2016. № 2. С. 73–132.

2. Диченко С.А. Модель угроз безопасности информации защищенных информационно-аналитических систем специального назначения // Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2022. № 1–2 (163–164). С. 64–71.

3. Кравченко А.Ю., Стукало Ю.Е. Проблемы и перспективы создания робототехнических комплексов военного назначения // Материалы VIII Всероссийской научно-практической конференции «Перспективные системы и задачи управления». 2013. С. 22–28.

4. Макаренко С.И. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 3. Радиоэлектронное подавление систем навигации и радиосвязи // Системы управления, связи и безопасности. 2020. № 2. С. 101–175.

5. Самойленко Д.В., Финько О.А. Обеспечение целостности информации в группе беспилотных летательных аппаратов в условиях деструктивных воздействий нарушителя // Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2017. № 5–6 (107–108). С. 20–27.

6. Забегалин Е.В. К вопросу об определении термина «информационно-техническое воздействие» // Системы управления, связи и безопасности. 2018. № 2. С. 121–150.

7. Сашников Т.К. К вопросу обеспечения информационной безопасности беспилотных авиационных систем с летательными аппаратами малого и легкого класса в специализированных АСУ // Сборник трудов Всероссийской научно-технической конференции «Теоретические и прикладные проблемы развития и совершенствования автоматизированных систем управления военного назначения». 2013. С. 247–251.

8. Диченко С.А., Финько О.А. Контроль и восстановление целостности многомерных массивов данных посредством криптокодовых конструкций // Программирование. 2021. № 6. С. 3–15.

9. Макаренко С.И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. № 3. С. 292–376.

References

1. Makarenko S.I. Robotic complexes for military purposes — the current state and development prospects // Systems of Control, Communication and Security. 2016. № 2. P. 73–132.

2. Dichenko S.A. A model of information security threats of protected special-purpose information and analytical systems // Voprosy oboronnoi tekhniki. Seriia 16. Tekhnicheskie sredstva protivodestviia terrorizmu. 2022. № 1–2 (163–164). P. 64–71.

3. Kravchenko A.Yu, Stukalo Yu.E. Problems and prospects of creating robotic military complexes. «Perspective systems and management tasks» // Materials of the eighth all-Russian scientific and practical conference. 2013. P. 22–28.

4. Makarenko S.I. Counter Unmanned Aerial Vehicles. Part 3. Electronic Warfare against Navigation and Radio Connection Subsystems of Unmanned Aerial Vehicles // Systems of Control, Communication and Security. 2020. № 2. P. 101–175.

5. Samoylenko D.V., Finko O.A. Providing integrity information group unmanned aerial vehicles under destructive impact pursue // Voprosy oboronnoi tekhniki. Seriia 16. Tekhnicheskie sredstva protivodestviia terrorizmu. 2017. № 5–6 (107–108). P. 20–27.

6. Zabegalin E.V. On the definition of the term «information technology impact // Systems of Control, Communication and Security. 2018. № 2. P. 121–149.

7. Sashnikov T.K. On the issue of ensuring information security of unmanned aerial systems with small and light class aircraft in specialized automated control systems // Proceedings of the All-Russian scientific and technical conference «Theoretical and applied problems of development and improvement of automated control systems for military purposes». 2013. P. 247–251.

8. Dichenko S.A., Finko O.A. Control and restoration of the integrity of multidimensional data arrays by means of cryptocode constructions // Programming. 2021. № 6. P. 3–15.

9. Makarenko S.I. Information weapons in the technical sphere: terminology, classification, examples // Systems of Control, Communication and Security. 2016. № 3. P. 292–376.