ПРИНЦИПЫ И МОДЕЛИ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСАХ ОТ ВНЕШНИХ ДЕСТРУКТИВНО-ИНФОРМАЦИОННЫХ ВОЗДЕЙСТВИЙ

Бардаев Э.А.¹, Винокуров А.В.², Задвижкин А.А.³, Колованов А.В.⁴, Лисицын В.В.⁵

Аннотация. Цель исследования заключается в защите информации, циркулирующей в робототехнических комплексах (РТК), и своевременном выявлении программно-аппаратных воздействий (ПАВ) злоумышленника на элементы критически важных систем (КВС) РТК. Предложены принципы защиты информации в РТК как составляющая теоретических основ обеспечения информационной безопасности (ИБ) РТК. На основе концептуальной модели информационного взаимодействия между подсистемами сегментов РТК выявлены особенности с точки зрения их рассмотрения как элементов эргодической системы, подверженных ПАВ злоумышленника. Проведена классификация угроз по стратегии нарушителя для достижения поставленной цели по нарушению информационной безопасности и устойчивости функционирования РТК. Проведено ранжирование угроз безопасности информации в РТК по величине потенциального ущерба. Формализована постановка научной задачи защиты информации в РТК в виде минимизации вероятности навязывания ложной информации или ее трансформации, а также минимизации вероятности необнаруживаемых ПАВ. Построены функциональная и математическая модели двухконтурной системы защиты информации в РТК: криптографической защиты информации и контроля целостности КВС. С целью эффективной и своевременной идентификации ПАВ предложен эпизодический контроль целостности элементов КВС в периоды отсутствия или сокращения нагрузки на вычислительные ресурсы систем обработки и защиты информационных потоков в РТК. Определены направления дальнейших исследований, заключающиеся в разработке новых методов и способов обработки и защиты информации в РТК.

Ключевые слова: программно-аппаратные воздействия, критически важные системы, контроль целостности, угрозы безопасности информации.

DOI: 10.21681/2311-3456-2019-6-49-58

Введение

Разработка и внедрение технологий военной робототехники является одним из приоритетных направлений создания новых и модернизации существующих на вооружении образцов вооружения и военной техники. В настоящее время практически во всех современных вооруженных конфликтах применяются робототехнические комплексы (РТК) [1-4]. Благодаря реализации государственного оборонного заказа и Государственной программы вооружения, ВС РФ имеют возможность осваивать и активно применять широкую номенклатуру наземных, морских и воздушных РТК военного назначения, основными областями применения которых являются: ведение разведки, прорыв обороны противника, обеспечение обороны роботизированными

огневыми точками, подавление огневого противодействия мобильными РТК, ликвидация нештатных ситуаций с опасными в обращении боеприпасами, обезвреживание взрывоопасных предметов, проведение аварийно-восстановительных работ, эвакуация с поля боя личного состава и техники под огнем, инженерная разведка, минирование и разминирование, обеспечение преодоления заграждений, доставка боеприпасов и материалов в зону огневого воздействия, охрана и оборона и др. [5, 6].

Одновременно с появлением новых типов РТК увеличивается количество угроз безопасности информации, циркулирующей в них, а наличие уязвимостей в протоколах взаимодействия сегментов РТК и приме-

- 1 Бардаев Эдуард Аркадьевич, доктор технических наук, старший научный сотрудник, сотрудник Восьмого управления Генерального штаба Вооруженных Сил Российской Федерации, г. Москва, Россия. E-mail: bardaev64@bk.ru
- 2 Винокуров Александр Владимирович, кандидат технических наук, доцент, профессор кафедры, Краснодарское высшее военное училище, г. Краснодар, Россия. E-mail: VAV73@rambler.ru
- 3 Задвижкин Алексей Анатольевич, адъюнкт, Краснодарское высшее военное училище, г. Краснодар, Россия. E-mail: z2a82@yandex.ru
- 4 Колованов Андрей Викторович, заместитель начальника Восьмого управления Генерального штаба Вооруженных Сил Российской Федерации, г. Москва, Россия. E-mail: z_357kl@mail.ru
- 5 Лисицын Василий Валерьевич, преподаватель кафедры, Краснодарское высшее военное училище, Краснодар, Россия. E-mail: lliiisss@list.ru

нение элементной базы и программного обеспечения зарубежного производства позволяют злоумышленнику осуществлять программно-аппаратные воздействия (ПАВ) на элементы критически важных систем (КВС) РТК [7-10].

Под деструктивными информационными воздействиями (ДИВ) будем понимать воздействия злоумышленника на радиоканалы и информацию средствами радиоэлектронной борьбы (РЭБ) и ПАВ на элементы КВС РТК [11].

Обеспечение информационной безопасности (ИБ) РТК в общей постановке проблемы может быть достигнуто путем [12]:

- защиты циркулирующей в РТК информации от дестабилизирующего воздействия внешних и внутренних угроз;
- защиты элементов РТК от дестабилизирующего воздействия внешних и внутренних информационных угроз;
- защиты внешней среды от информационных угроз со стороны РТК.

В условиях ПАВ параметры КВС выходят за допустимые пределы или меняют свои значения, что приводит не только к нарушению ИБ РТК, но и к нарушению устойчивости функционирования соответствующей КВС и РТК в целом, а также может привести к переходу РТК в качестве субъекта угроз, например, их использования в террористических целях [13, 14].

Цель статьи заключается в защите информации, циркулирующей в РТК, и своевременном выявлении ПАВ злоумышленника на элементы КВС РТК путем построения моделей системы защиты информации в виде контуров криптографической защиты информации и контроля целостности элементов КВС РТК от ПАВ злоумышленника.

Принципы защиты информации в РТК

С учетом стоимости РТК и возможных последствий и величины ущерба, возникающего при реализации злоумышленником ДИВ, предлагаются следующие основные идеи, соответствующие целям обеспечения ИБ и устойчивости функционирования РТК с учетом удовлетворения потребностей надсистем, в интересах которых они разрабатываются и функционируют:

- обеспечение качества информации, циркулирующей в РТК и удовлетворяющей предъявляемым требованиям;
- обеспечение непрерывности защиты информации в РТК на протяжении технологических циклов их функционирования и оперативного реагирования на появление новых уязвимостей;
- обеспечение адекватности мер защиты информации условиям функционирования РТК и внешним деструктивным воздействиям.

Каждая идея конкретизируется совокупностью принципов защиты информации в РТК.

Принцип конечной цели. Главной целью построения системы защиты информации РТК является достижение максимальной эффективности функционирования РТК. Защита информации не должна ухудшать целевую

функцию РТК в интересах надсистемы с сохранением требуемого качества информации, где под качеством понимается не только обеспечение защищенности, но и ценности. Данный принцип согласуется с одним из основных принципов защиты информации, определяющим, что затраты на систему защиты не должны превышать стоимость защищаемой информации.

Принцип обоснованности защиты информации заключается в определении информационных потоков, подлежащих защите, установлении их степени секретности, нахождении компромисса при выборе методов и средств защиты исходя из выделяемых ресурсов.

Принцип комплексности защиты. Комплексное применение мер защиты от угроз информационной безопасности РТК может быть достигнуто при взаимосоглазованном участии в решении соответствующих задач всего персонала, который организует и осуществляет процессы сбора, передачи, хранения, обработки и использования информации, а также осуществляет эксплуатацию и обслуживание сегментов РТК.

Принцип целевой эффективности системы защиты информации предполагает более углубленный анализ угроз безопасности информации в РТК. После оценки уязвимостей и выявления возможных угроз следует провести анализ влияния этих угроз на значения защищаемых показателей качества и комплексно применять меры защиты только против угроз, деструктивно влияющих на значения защищаемых показателей, и только в той мере, в которой они способны повлиять на качество информации.

Принцип взаимосвязи данных. Наличие логических связей между информационными потоками РТК позволяет злоумышленнику снизить качество одного из видов информации, воздействуя на другие, возможно менее защищенные в определенный момент времени. Если у злоумышленника есть множество вариантов воздействий на информационные потоки, с различными уровнями защищенности, то он выберет для воздействия наименее защищенные.

Принцип гарантированного результата. Система защиты информации должна обеспечивать требуемое качество информации в любых условиях, включая неопределенность влияющих факторов.

Принцип превентивности принимаемых мер по защите информации предполагает априорное заблаговременное принятие мер по защите информации в ходе разработки РТК до начала обработки информации.

Принцип связности предполагает рассматривать систему защиты информации во взаимодействии с системой управления РТК, в зависимости от связей объекта защиты с внешней средой, с вышестоящими, нижестоящими системами, а также внутренними связями между подсистемами (элементами).

Принцип комплексирования заключается в логическом и технологическом объединении подсистем и модулей, выполняющих задачи по обработке и защите разнородных потоков информации, в унифицированных устройствах.

Принцип единства мер защиты. Подсистемы и элементы РТК должны участвовать в достижении ин-

тегративного эффекта, чтобы их качественные и функциональные характеристики повышали эффективность системы в целом.

Принцип функциональности. Если существующая организационная, технологическая, управленческая структура РТК не позволяет обеспечить требуемые функциональные возможности, то такая структура должна быть изменена (оптимизирована).

Принцип развития. Технологические и конструкторские решения должны предусматривать возможности наращивания, модернизации, расширения качественных и функциональных характеристик системы защиты информации с целью обеспечения длительной по времени адекватности поставленным задачам.

Принципы уровневой структуры защиты. Защищенность информации должна обеспечиваться на всех этапах ее обработки, а система защиты информации должна строиться путем обеспечения услуг защиты на нескольких уровнях.

Следует выделить, что РТК различного назначения представляют собой сложные эргодические системы, которые характеризуется следующими особенностями с точки зрения их рассмотрения как объектов, подверженных ДИВ злоумышленника:

- наличие сложных взаимосвязей между разнородными информационными потоками, функционирующие внутри РТК ними, например, снижение имитозащищенности командно-программной информации (КПИ), определяющей устойчивость управления РТК, может привести к переходу РТК в объект угроз; ДИВ на телеметрическую информация может привести к формированию ложных

команд управления РТК и нарушению их функциональной устойчивости; ДИВ на инерциально-навигационную систему, интегрированную с высокоточной спутниковой аппаратурой и системой машинного зрения может привести к нарушению достоверности специальной информации и т.д.;

- наличие разнородных по структуре, формату и избыточности видов информации предполагает применение криптографических средств защиты информации и специальных протоколов передачи данных;
- массогабаритные и энергетические ограничения РТК определяют дополнительные требования к средствам обнаружения ДИВ и защиты систем РТК и информации, функционирующей в них.

Концептуальная модель информационного взаимодействия между подсистемами сегментов РТК представлена на (рис. 1).

Модель угроз безопасности информации и функциональной устойчивости РТК

Так как модель обнаружения вторжений должна строиться на базе классификации угроз и учитывать структуру и фазы проведения атаки на РТК, определять источники и цели атаки, то проведем классификацию угроз по стратегии нарушителя для достижения поставленной цели:

первого типа направлены на установление (раскрытие) языка информационного обмена БЛА-НПУ; цель – получить специальную информацию КБЛА (данные разведки, интеллектуальной СПР, команды управления в рамках боевой информационной системы);

второго типа направлены на навязывание ложной информации; в данном случае предполагается навязыва-

Рис. 1. Концептуальная модель информационного взаимодействия между подсистемами сегментов РТК

вание ложных команд управления с наземных пунктов управления, а также перехват и целенаправленное искажение навигационных данных (спуфинг-атака); цель – перехват управления БЛА, навязывание ложной специальной информации;

третьего типа направлены на срыв или ухудшение качества информационных взаимодействий путем создания агрессивной среды осуществления информационных взаимодействий, что достигается, например, при постановке помех средствами радиоэлектронного подавления и др.; цель – затруднить или нарушить управление БЛА, искажение целевой информации;

четвертого типа направлены на нарушение целостных характеристик систем обработки и защиты информации, а также других КВС; данные стратегии могут ис-

пользоваться, когда отсутствуют возможности по реализации вышестоящих типов стратегий; цель – нанесение ущерба системам РТК путем ПАВ. При этом результатом воздействия является нарушение тех же составляющих информационной безопасности (конфиденциальности, целостности и доступности), которые рассмотрены в стратегиях 1-3, а также нарушение устойчивости функционирования РТК.

Распределение сценариев нарушителя в соответствии с уровнями и типами стратегий приведено в таблице 1.

Построим модель «с полным перекрытием», представляющую собой триаду «угрозы – уязвимости – объекты защиты» в виде трехдольного графа (рис. 2).

Таблица 1

Реляционное представление стратегий противника

Уровень	Тип стратегии	Сценарий нарушителя
Стратегия 1 типа	Нарушение конфиденциальности	Компрометация ключевой документации на НПУ и РТК. Перехват и дешифрование информации. Вскрытие шифра в результате криптоанализа.
Стратегия 2 типа	Нарушение имитостойкости	Вскрытие алгоритма и ключа обеспечения имитостойкости. Навязывание ложных команд управления БЛА, СИ, ТМИ и навигационных данных.
Стратегия 3 типа	Нарушение достоверности и доступности	Радиоэлектронное подавление команд управления БЛА, СИ, ТМИ и навигационных данных. Нарушение правил вхождения в связь. Срыв синхронизации сеанса.
Стратегия 4 типа	Нарушение сохранности (работоспособности) элементов и подсистем РТК	Внедрение закладочных устройств и РПВ. Модификация ПО. Подмена, уничтожение, хищение наиболее важных компонентов КБЛА. Воздействие на элементы инфраструктуры: электропитание, линии связи и т.д.

Рис. 2. Модель «угрозы – уязвимости – объекты защиты»

Таким образом (см. рис.2), имеем множества:
 $Y=\{y_i\}$ – множество угроз безопасности;
 $O=\{o_i\}$ – множество объектов (ресурсов) защищенного РТК;

$X=\{x_i\}$ – множество уязвимых мест РТК, определяемое подмножеством декартова произведения $Y \times O$: $x_i = \langle y_i, o_i \rangle$.

Выбор множества механизмов защиты $S=\{s_i\}$ определяется целью перекрытия всех возможных ребр в графе $\langle Y, X, O \rangle$.

Как показано в табл. 1, предложенная классификация угроз по стратегии нарушителя для достижения поставленной цели определяет цели воздействия, которые коррелируют со свойствами безопасности информации, что позволяет в дальнейшем синтезировать систему защиты с оптимизацией данных параметров.

Реализовать угрозы противник может на всех логических уровнях обработки информации в РТК. Для обоснованного применения механизмов защиты необходимо оценить уровень угроз на информационное

обеспечение РТК. В таблице представлены результаты ранжирования угроз безопасности информации по величине потенциального ущерба.

Построение модели системы защиты информации и контроля целостности КВС путем идентификации ПАВ на их элементы

На основании анализа угроз безопасности информации в РТК можно выделить следующие закономерности:

1. Несмотря на разнообразие возможных внешних ДИВ злоумышленника их можно сгруппировать по объекту воздействия:

радиоканалы и информация, циркулирующая в них; критически важные элементы систем РТК.

2. Наибольший ущерб наносят ДИВ, направленные на навязывание ложной информации или скрытые ПАВ, которые не обнаруживает система защиты РТК.

Рассмотрим типовую функциональную структуру РТК с выделением информационных потоков (рис. 3).

Ранжирование угроз РТК по величине потенциального ущерба

Таблица 2

Уровень	Угрозы	Степень угрозы
1	Раскрытие содержания телеметрической информации	Малая
2	Раскрытие протоколов взаимодействия	Малая
3	Раскрытие содержания командно-программной информации	Средняя
4	Искажение телеметрической информации	Средняя
5	Искажение навигационного поля	Средняя
6	Подавление командной информации	Средняя
7	Раскрытие содержания специальной информации, ограниченного распространения	Высокая
8	Навязывание ложного навигационного поля	Высокая
9	Навязывание ложной командно-программной информации	Высокая
10	Нарушение функционирования критически важных систем	Высокая

Рис. 3. Внутренняя функциональная структура РТК

В представленной структуре РТК (см. рис. 3) выделены следующие системы, которые можно отнести к КВС:

- защиты информации;
- навигации и точного времени;
- обработки данных;
- управления РТК и целевыми нагрузками;
- приема-передачи данных.

Наличие информационных связей между системами при реализации злоумышленником ПАВ на отдельные их элементы может привести к размножению ошибки и нарушению параметров взаимодействующих систем.

С учетом величины потенциального ущерба при реализации злоумышленником угроз (см. табл. 2) сформулируем задачу защиты информации и функциональной устойчивости РТК в виде оптимизационной задачи:

$$\left\{ \begin{array}{l} X(u^*(V, R)) \rightarrow \min_{u \in U(V, R)} \\ u(v_i) = f(v_i) \\ u(r_j) = f(r_j) \\ X(u^*(v_i)) = \langle P_{\text{нав}}, P_{\text{тр}} \rangle, \\ X(u^*(r_j)) = (P_{\text{необ.ПАВ}}) \\ t(v_i) \leq t(v_i)_{\text{доп}} \\ t(r_j) \leq t(r_j)_{\text{доп}} \end{array} \right. \quad (1)$$

где: X – множество значений показателей эффективности системы защиты информации и обнаружения ПАВ, $V = \{v_i, i=1, \dots, 4\}$ – вид информации в РТК (V_1 – навигационная, V_2 – телеметрическая; V_3 – командно-программная, V_4 – специальная), $R = (r_1, r_2, \dots, r_j)$ – вектор контролируемых элементов КВС, $u(v_i)$ – стратегии по защите i -го вида информации, $u(r_j)$ – стратегии по об-

наружению ПАВ на j -й элемент КВС; $P_{\text{нав}}$ – вероятность навязывания ложной информации, $P_{\text{тр}}$ – вероятность трансформации информации, $P_{\text{необ.ПАВ}}$ – вероятность необнаруживаемых ПАВ; $t(v_i)$ – время идентификация ДИВ на V информацию i -го вида; $t(v_i)_{\text{доп}}$ – допустимое время идентификации ДИВ на V информацию i -го вида до ее доведения до потребителя (ЛПР); $t(r_j)$ – время идентификация ПАВ на j -е элементы КВС; $t(r_j)_{\text{доп}}$ – допустимое время идентификация ПАВ на j -е элементы КВС до выполнения функциональной задачи соответствующей системой РТК.

Необходимость выполнения типовых функций контроля целостности информации и КВС, а также наличие влияния защищенности информации на устойчивость функционирования РТК позволяет выдвинуть гипотезу о возможности объединения процессов защиты информации в РТК и идентификации ПАВ на элементы КВС РТК в рамках интегрированной системы защиты информации, включающей логически взаимосвязанные подсистемы контроля целостности: навигационной информации (НИ), командно-программной информации (КПИ) и телеметрической информации, элементов КВС.

Рассмотрим модель системы защиты информации и контроля целостности (рис. 4).

В соответствии с предложенной моделью защита информации в условиях ДИВ на информацию, циркулирующую в радиопереносных, и ПАВ на КВС РТК сводится к описанию соответствующего вектора уравнениями:

$$S_{\text{зи}}(V, R) = f(S, C, t_d, t(v), t(r)), \quad (2)$$

где: $S = (s_1, s_2, \dots, s_z)$ – вектор состояний СЗИ, $C = (c_1, c_2, c_3, c(r_1), c(r_2), \dots, c(r_j))$ – вектор реакций на ДИВ на информацию и ПАВ на элементы КВС, t_d – время действия атаки, $t(v) = (t_p + t_{\text{па}})$ – время защиты информации от ДИВ, включая время реакции на ДИВ t_p и время противодействия атаки $t_{\text{па}}$, $t(r)$ – время реакции на ПАВ на элементы КВС и их локализацию (устранение последствий или выработка блокирующих сигналов).

Рис. 4. Функциональная модель системы защиты информации РТК и контроля целостности КВС

С целью эффективной и своевременной идентификации ПАВ предлагается эпизодический контроль целостности элементов КВС в периоды отсутствия или сокращения нагрузки на вычислительные ресурсы систем обработки и защиты информационных потоков в РТК. Вид РТК, архитектура вычислителя и возможности его задействования на решение задач защиты информации определяют реализацию применения последовательной или параллельной идентификации ПАВ на КВС.

Решение поставленной задачи (1) в условиях ограничения вычислительных и энергетических ресурсов, характерных для РТК, может быть достигнуто за счет:

- модернизации методов обнаружения и противодействия компьютерным атакам, предложенных в работе [15], и их адаптации с учетом особенностей РТК как объекта ПАВ;
- применения методов и способов крипто- и имитозащиты информации, позволяющих выявлять факты навязывания ложной информации и их идентифицировать на фоне помех в радиоканалах, например, предложенных в работах [16-18];
- разработки методов и способов контроля целостности навигационной информации с учетом имеющихся научных исследований в данной области, например, за счет применения корреляционно-экстремальных-навигационных систем [19];
- совмещения функций криптозащиты и сжатия информации в одной подсистеме или функциональном устройстве [20-24].

Заключение

Предъявляемые к РТК требования по функциональному использованию и их массогабаритные и энергетиче-

ские ограничения не позволяют в настоящее время полностью отказаться от применения технологий и элементной базы иностранного производства, что позволяет злоумышленнику помимо ДИВ на радиоканалы и информацию использовать уязвимости в системах РТК.

На основе наличия информационных взаимосвязей между системами РТК предложено объединение процессов контроля защиты информации в РТК и идентификации ПАВ на элементы КВС в рамках единой системы защиты информации, что должно повысить эффективность защиты информации в РТК и обеспечить их функциональную устойчивость в рамках ограниченных массогабаритных и энергетических ресурсов.

На основе проведенного анализа угроз безопасности информации сформулирована математическая постановка задачи и построена функциональная модель системы защиты информации и контроля целостности КВС путем идентификации ПАВ на их элементы.

Для повышения эффективности защиты информации в РТК, функционирующих в условиях ДИВ злоумышленника, обоснована необходимость решения следующих задач:

- конкретизация моделей угроз безопасности информации в РТК в соответствии с их типом и условиями функционирования;
- формирование перечня КВС и ключевых элементов РТК;
- определение периодичности контроля целостности программно-аппаратного обеспечения КВС РТК;
- исследование уязвимостей операционных систем специального назначения, применяемых в РТК.

Литература

1. Безденежных С.И., Брайткрайц С.Г., Репников Д.А. и др. Эволюционно-технологический подход в управлении требованиями к робототехническим комплексам военного назначения // Вестник СибГУТИ. 2019. № 2. С. 87-93.
2. Иванов С.С. Задачи, решаемые перспективными робототехническими комплексами военного назначения сухопутных войск и требования к ним / С.С. Иванов, П.А. Дутьнев, А.В. Воронович // Труды военно-научной конференции «Роботизация Вооруженных Сил Российской Федерации», Москва, 2016. С. 28-32.
3. Корсунский В.А. Перспективы развития военных мобильных робототехнических комплексов наземного базирования в России / В.А. Корсунский, В.Н. Наумов // Вестник МГТУ им. Н.Э. Баумана: электронное издание, 2013.
4. Кравченко А.Ю. Проблемы и перспективы создания робототехнических комплексов военного назначения / А.Ю. Кравченко, Ю.Е. Стукало // Материалы VIII Всероссийской научно-практической конференции «Перспективные системы и задачи управления», 2013. – С. 22-48.
5. Мосиенко С.А. Концепция построения наземного робототехнического ударного комплекса / С.А. Мосиенко, В.И. Лохтин – М.: «САМПОЛИГРАФИСТ», издание 2-е, дополненное, 2014. – 122 с.
6. Рудянов Н.А., Хрущёв В.С. Концептуальные вопросы построения и применения автономных робототехнических комплексов военного назначения // Военная мысль. 2019. № 6. С. 55-61.
7. Винокуров А.В. Анализ угроз безопасности информации, обрабатываемой в комплексах с беспилотными летательными аппаратами / А.В. Винокуров, А.А. Задвижкин // Информационная безопасность – актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности: матер. XVII Всерос. межведомст. НТК, 2018 г.; отв. ред. д.т.н., проф. А.В. Крупенин. – Краснодар : КВВУ, 2018. – С. 123-127.
8. Гонтарь Д.Н., Шибанов В.Е., Петрунин Д.В. Определение и анализ уязвимостей робототехнических комплексов военного назначения // Альманах мировой науки. 2018. № 6 (26). С. 17-19.
9. Леонов А.В., Тюлькин М.В., Трущенко В.В. Критерии оценки целесообразности и эффективности использования робототехнических комплексов военного назначения // Вооружение и экономика. 2019. № 1 (47). С. 23-29.

10. Новиков А.В., Зевин В.В., Расщепкин И.А. Проблемы эксплуатации робототехнических комплексов военного назначения воздушного применения в Вооруженных Силах Российской Федерации // Военная мысль. 2018. № 7. С. 80-84.
11. Шеремет И.А. Противодействие информационным и кибернетическим угрозам // Вестник академии военных наук. 2016. № 2 (55). С. 29-34.
12. Винокуров, А.В. Обеспечение информационной безопасности комплексов с беспилотными летательными аппаратами как задача противодействия терроризму / Научно-технический журнал «Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму», вып. 9-10 (11-112), 2017. – С. 66-70.
13. Винокуров, А.В. Техносферная безопасность комплексов с беспилотными летательными аппаратами // Технологии техносферной безопасности. Вып. 6 (76). 2017. – Режим доступа: <http://academygps.ru/ttb>. (дата обращения 02.04.2017).
14. Кузнецов Ю.В. Винокуров А.В., Бардаев Э.А. Теоретические основы обеспечения информационной безопасности робототехнических комплексов // Военная мысль. 2018. № 12. С. 71-78.
15. Климов, С.М. Методы и модели противодействия компьютерным атакам. – Люберцы : КАТАЛИТ, 2008. – 316 с.
16. Винокуров А.В. Защита командно-программной информации управления беспилотными летательными аппаратами / А.В. Винокуров, М.И. Бухонский, Г.И. Дейкун / Инновационные технологии в образовательном процессе – Материалы XIX Всероссийской научно-практической конференции. – Краснодар: КВВАУЛ, 2017. – С.38-45.
17. Овчаренко М.В. Методологические основы построения имитостойчивой аппаратуры передачи данных / М.В. Овчаренко, А.В. Винокуров // Информационные ресурсы России, 2015. – № 5. – С. 38-41.
18. Патент 164498 Российская Федерация, МПК7 G 09 C 1/00, H 03 M 13/23. Устройство имитостойкого кодирования / А.В. Винокуров, М.В. Овчаренко; заявитель и патентообладатель КВВУ имени генерала армии С.М. Штеменко. – № 20155141723; заявл. 30.09.2015; опубл. 10.09.2016, Бюллетень № 25. – 2 с.
19. Сырямкин, В.И. Корреляционно-экстремальные радио-навигационные системы / В.И. Сырямкин, В.С. Шидловский – Томск: Изд-во Томского ун-та, 2010. – 316 с.
20. Цветков, В.В. Устойчивый к канальным ошибкам видеокодек подвижных изображений на основе трехмерного ортогонального преобразования с обеспечением конфиденциальности и аутентификации передаваемых видеоданных / В.В. Цветков, А.А. Устинов, И.Н. Оков. – М.: Информация и космос. – 2015. – № 2. – С. 52-59.
21. Nasrullah, Sang J, Akbar MA, Cai B, Xiang H, Hu H. Joint image compression and encryption using IWT with SPIHT, Kd-tree and chaotic maps // Applied Sciences. 2018. Vol. 8(10). doi:10.3390/app8101963.
22. Agarwal S. Secure Image Transmission Using Fractal and 2D-Chaotic Map // Journal of Imaging. 2018. Vol. 4(1). doi:10.3390/jimaging4010017.
23. Younas I, Khan M. A New Efficient Digital Image Encryption Based on Inverse Left Almost Semi Group and Lorenz Chaotic System // Entropy. 2018. Vol. 20(12). doi:10.3390/e20120913.
24. Патент 2595953 Российская Федерация, МПК7 H 04 L 9/00 Способ арифметического кодирования с шифрованием / В.Б. Васильев [и др.]; заявитель и патентообладатель – Акционерное общество «Концерн радиостроения «Вега»; заявл. 04.08.2015; опубл. 27.08.2016, Бюл. № 24.

PRINCIPLES AND MODELS USED TO CREATE INFORMATION SECURITY SYSTEMS IN ROBOTIC SYSTEMS TO PROTECT THE INFORMATION FROM EXTERNAL DESTRUCTIVE INFORMATION INFLUENCE

Bardaev E.A.⁶, Vinokurov A.V.⁷, Zadvizhkin A.A.⁸, Kolovanov A.V.⁹, Lisitsyn V.V.¹⁰

Principles of information protection in robotic systems have been suggested as part of the theoretical basis for assuring the information security of the robotic systems. Information security threats in robotic systems have been analyzed and threats have been identified which are the most important in terms of damage inflicted on robotic

6 Eduard Bardaev, Dr.Sc. (Tech.), General Staff of the Armed Forces of the Russian Federation, Moscow, Russia. E-mail: bardaev64@bk.ru

7 Alexander Vinokurov, Ph.D., Associate Professor, Krasnodar Higher Military School, Krasnodar, Russia. E-mail: VAV73@rambler.ru

8 Alexey Zadvizhkin, Krasnodar Higher Military School, Krasnodar, Russia. E-mail: z2a82@yandex.ru

9 Andrey Kolovanov, Deputy Head of the Supreme Directorate of the General Staff of the Armed Forces of the Russian Federation, Moscow, Russia. E-mail: z_357kl@mail.ru

10 Vasily Lisitsyn, Krasnodar Higher Military School, Krasnodar, Russia. E-mail: liliiss@list.ru

systems. Scientific problem statement has been formalized for information protection in robotic systems in terms of minimizing the probability of false information imposing or its transformation, as well as minimizing the probability of unidentifiable software and hardware impacts. Functional and mathematical models of double loop information security system in robotic systems have been created – the loop of cryptographic information protection and that of the critical systems integrity monitoring. The hypothesis has been substantiated that it is possible to ensure the required information security and continuity of robotic systems by casual control of critical system elements integrity in the periods when the load on computational resources of the information flows processing and protection system in the robotic systems is missing or reduced.

Keywords: hardware and software impacts, critical systems, integrity control, information security threats.

References

1. Bezdenezhnyh S.I., Brajtkrajc S.G., Repnikov D.A. i dr. Evolyucionno-tehnologicheskij podhod v upravlenii trebovaniyami k robototekhnicheskim kompleksam voennogo naznacheniya // Vestnik SibGUTI. 2019. № 2. S. 87-93.
2. Ivanov S.S. Zadachi, reshaemye perspektivnymi robototekhnicheskimi kompleksami voennogo naznacheniya suhoputnyh vojsk i trebovaniya k nim / S.S. Ivanov, P.A. Dul'nev, A.V. Voronovich // Trudy voenno-nauchnoj konferencii «Robotizaciya Vooruzhennyh Sil Rossijskoj Federacii», Moskva, 2016. – S. 28-32.
3. Korsunskij V.A. Perspektivy razvitiya voennyh mobil'nyh robototekhnicheskikh kompleksov nazemnogo bazirovaniya v Rossii / V.A. Korsunskij, V.N. Naumov // MGTU im. N.E. Bauman, Moskva, Vestnik MGTU im. N.E. Bauman: elektronnoe izdanie, 2013.
4. Kravchenko A.YU. Problemy i perspektivy sozdaniya robototekhnicheskikh kompleksov voennogo naznacheniya / A.YU. Kravchenko, YU.E. Stukalo // Materialy VIII Vserossijskoj nauchno-prakticheskoy konferencii «Perspektivnye sistemy i zadachi upravleniya», 2013. – S. 22-48.
5. Mosienko S.A. Konceptiya postroeniya nazemnogo robototekhnicheskogo udarnogo kompleksa / S.A. Mosienko, V.I. Lohtin – M.: «SAMPOLIGRAFIST», izdanie 2-e, dopolnennoe, 2014. – 122 s.
6. Rudianov N.A., Hrushchyov V.S. Konceptual'nye voprosy postroeniya i primeneniya avtonomnyh robototekhnicheskikh kompleksov voennogo naznacheniya // Voennaya mysl'. 2019. № 6. S. 55-61.
7. Vinokurov A.V. Analiz ugroz bezopasnosti informacii, obrabatyvaemoj v kompleksah s bespilotnymi letatel'nymi apparatami / A.V. Vinokurov, A.A. Zadvizhkin // Informacionnaya bezopasnost' – aktual'naya problema sovremennosti. Sovershenstvovanie obrazovatel'nyh tekhnologij podgotovki specialistov v oblasti informacionnoj bezopasnosti: mater. HVII Vseros. mezhvedomst. NTK, 2018 g.; otv. red. d.t.n., prof. A.V. Krupenin. – Krasnodar : KVVU, 2018. – S. 123-127.
8. Gontar' D.N., SHibanov V.E., Petrulin D.V. Opredelenie i analiz uyazvimostej robototekhnicheskikh kompleksov voennogo naznacheniya // Al'manah mirovoj nauki. 2018. № 6 (26). S. 17-19.
9. Leonov A.V., Tyul'kin M.V., Trushchenkov V.V. Kriterii ocenki celesoobraznosti i effektivnosti ispol'zovaniya robototekhnicheskikh kompleksov voennogo naznacheniya // Vooruzhenie i ekonomika. 2019. № 1 (47). S. 23-29.
10. Novikov A.V., Zevin V.V., Rasshchepkin I.A. Problemy ekspluatatsii robototekhnicheskikh kompleksov voennogo naznacheniya vozdušnogo primeneniya v Vooruzhennyh Silah Rossijskoj Federacii // Voennaya mysl'. 2018. № 7. S. 80-84.
11. SHeremet I.A. Protivodejstvie informacionnym i kiberneticheskim ugrozam // Vestnik akademii voennyh nauk. 2016. № 2 (55). S. 29-34.
12. Vinokurov, A.V. Obespechenie informacionnoj bezopasnosti kompleksov s bespilotnymi letatel'nymi apparatami kak zadacha protivodejstviya terrorizmu / Nauchno-tehnicheskij zhurnal «Voprosy oboronnoj tekhniki. Seriya 16. Tekhnicheskie sredstva protivodejstviya terrorizmu», vyp. 9-10 (11-112), 2017. – S. 66-70.
13. Vinokurov, A.V. Tekhnosfernaya bezopasnost' kompleksov s bespilotnymi letatel'nymi apparatami // Tekhnologii tekhnosfernoj bezopasnosti. Vyp. 6 (76). 2017. – Rezhim dostupa: <http://academygps.ru/ttb>. (data obrashcheniya 02.04.2017).
14. Kuznecov YU.V. Vinokurov A.V., Bardaev E.A. Teoreticheskie osnovy obespecheniya informacionnoj bezopasnosti robototekhnicheskikh kompleksov // Voennaya mysl'. – 2018. – № 12. – S. 71-78.
15. Klimov, S.M. Metody i modeli protivodejstviya komp'yuternym atakam. – Lyubercy : KATALIT, 2008. – 316 s.
16. Vinokurov A.V. Zashchita komandno-programmnoj informacii upravleniya bespilotnymi letatel'nymi apparatami / A.V. Vinokurov, M.I. Buhonskij, G.I. Dejkun / Innovacionnye tekhnologii v obrazovatel'nom processe Materialy XIX Vserossijskoj nauchno-prakticheskoy konferencii. – Krasnodar: KVVAUL, 2017. – S.38-45.
17. Ovcharenko M.V. Metodologicheskie osnovy postroeniya imitoustojchivoj apparatury peredachi dannyh / M.V. Ovcharenko, A.V. Vinokurov // Informacionnye resursy Rossii, 2015. – № 5. – S. 38-41.
18. Pat. 164498 Rossijskaya Federaciya, MPK7 G 09 S 1/00, H 03 M 13/23. Ustrojstvo imitostojkogo kodirovaniya / A.V. Vinokurov, M.V. Ovcharenko; zayavitel' i patentoobladatel' KVVU imeni generala armii S.M. SHtemenko. – № 20155141723 ; zayavl. 30.09.2015; opubl. 10.09.2016, Byul. № 25. – 2 s.
19. Syryamkin, V.I. Korrelyacionno-ekstremal'nye radio-navigacionnye sistemy / V.I. Syryamkin, V.S. SHidlovskij – Tomsk: Izd-vo Tom. un-ta, 2010. – 316 s.
20. Cvetkov, V.V. Ustojchivyy k kanal'nym oshibkam videokodek podvizhnyh izobrazhenij na osnove trekhmernogo ortogonal'nogo preobrazovaniya s obespecheniem konfidencial'nosti i autentifikacii peredavaemyh videodannyh / V.V. Cvetkov, A.A. Ustinov, I.N. Okov. – M.: Informaciya i kosmos. – 2015. – № 2. – S. 52-59.
21. Nasrullah, Sang J, Akbar MA, Cai B, Xiang H, Hu H. Joint image compression and encryption using IWT with SPIHT, Kd-tree and chaotic maps // Applied Sciences. 2018. Vol. 8(10). doi:10.3390/app8101963.

22. Agarwal S. Secure Image Transmission Using Fractal and 2D-Chaotic Map // Journal of Imaging. 2018. Vol. 4(1). doi:10.3390/jimaging4010017.
23. Younas I, Khan M. A New Efficient Digital Image Encryption Based on Inverse Left Almost Semi Group and Lorenz Chaotic System // Entropy. 2018. Vol. 20(12). doi:10.3390/e20120913.
24. Pat. 2595953 Rossijskaya Federaciya, MPK7 H 04 L 9/00 Sposob arifmeticheskogo kodirovaniya s shifrovaniem / V.B. Vasil'ev [i dr.]; zayavitel' i patentoobladatel' – Akcionernoe obshchestvo «Koncern radiostroeniya «Vega»; zayavl. 04.08.2015; opubl. 27.08.2016, Byul. № 24.