УДК 621.394.6
ГРНТИ 78.25.13

ЗАДАЧИ И НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ВОЕННОГО И ДВОЙНОГО НАЗНАЧЕНИЯ ОТ ПРЕДНАМЕРЕННЫХ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ

Е.А. ЖИДКО, доктор технических наук, доцент
Воронежский государственный технический университет (г. Воронеж)
С.С. КУЩЕВ, кандидат технических наук, доцент
ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)
С.Н. РАЗИНЬКОВ, доктор физико-математических наук, старший научный сотрудник
ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)
С.В. ТЕНЯЧКИН
ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)

Проведен анализ задач и направлений совершенствования защиты информационно-телекоммуникационных систем военного и двойного назначения от преднамеренных деструктивных воздействий, создаваемых программными средствами несанкционированного доступа в информационные области и комплексами радиоэлектронной борьбы, нарушающими процессы передачи-приема и обработки информации путем постановки маскирующих или имитирующих помех. Исследованы возможности и условия применения методов адаптивного, ситуационного и рефлексивного управления информационным ресурсом защищаемой системы. Определена рациональная стратегия организации защиты в интересах достижения безопасности информации и информационной инфраструктуры при регламентированных изменениях показателей эффективности информационного обмена в информационно-телекоммуникационных системах.

Ключевые слова: информационно-телекоммуникационная система, преднамеренное деструктивное воздействие, информационный ресурс, безопасность информации и информационной инфраструктуры, методы адаптивного, ситуационного и рефлексивного управления.

TASKS AND DIRECTIONS FOR IMPROVING THE PROTECTION OF MILITARY AND DUAL-USE PURPOSES INFORMATION AND TELECOMMUNICATIONS SYSTEMS FROM DELIBERATE DESTRUCTIVE INFLUENCES

E.A. ZHIDKO, Doctor of Technical Sciences, Associate Professor
Voronezh State Technical University (Voronezh)
S.S. KUSCHEV, Candidate of Technical Sciences, Associate Professor
MESC AF «N.E. Zhukovsky and Y.A. Gagarin Air Force Academy» (Voronezh)
S.N. RAZINKOV, Doctor of Physical and Mathematical Sciences, Senior Researcher
MESC AF «N.E. Zhukovsky and Y.A. Gagarin Air Force Academy» (Voronezh)
S.V. TENYACHKIN
MESC AF «N.E. Zhukovsky and Y.A. Gagarin Air Force Academy» (Voronezh)

The analysis of the tasks and directions of improving the protection of military and dual-use information and telecommunications systems of against deliberate destructive influences created by software tools of unauthorized access to information areas and electronic warfare complexes that

СОДЕРЖАНИЕ

violate the processes of transmitting, receiving and processing information by setting masking or simulating interference is carried out. The possibilities and conditions of using the protected system information resource adaptive, situational and reflexive management methods are investigated. The rational strategy of the protection organization in the interests of achieving the security of information and information infrastructure with regulated changes in the performance indicators of information exchange in information and telecommunications systems is defined.

Keywords: information and telecommunications system, deliberate destructive impact, information resource, security of information and information infrastructure, methods of adaptive, situational and reflexive management.

Введение. В соответствии с Концепцией борьбы с системами боевого управления C^3CM – Command, Control and Communication Counter Measures [1, 2] одной из важнейших задач по завоеванию превосходства в управлении в перспективных военных действиях с участием армии США и Объединенных вооруженных сил НАТО является дезорганизация управления войсками (силами) и оружием противника. В результате ее выполнения достигается упреждение в принятии оперативных (боевых) решений, обеспечивающее сосредоточение усилий и наращивание группировок войск (сил) на важнейших направлениях, а также повышение эффективности защиты критически важных объектов [2, 3] от массированных ракетно-авиационных (огневых) ударов [1, 4].

Степень дезорганизации управления войсками (силами) и оружием в значительной мере будет определяться эффективностью преднамеренных деструктивных воздействий (ДВ) на информационно-телекоммуникационные системы (ИТС) военного и двойного назначения (ВДН) для автоматизированных систем управления (АСУ) с применением комплексов (средств) информационного противоборства (ИПБ).

Для создания преднамеренных ДВ на ИТС ВДН применяются:

программные средства несанкционированного доступа в информационные области ИТС в целях нарушения процедур передачи-приема, обработки, уничтожения или подмены информации для АСУ [5–7];

комплексы радиоэлектронной борьбы, создающие маскирующие или имитирующие помехи [8, 9] для дестабилизации условий передачи-приема информации в каналах связи [10, 11]. Маскирующие помехи нарушают нормальные условия информационного обмена за счет энергетического подавления полезных сигналов (снижения отношения сигнал-шум) на входе приемников; в результате их создания возникают ошибки передачи-приема и обработки информации в ИТС. Имитирующие помехи, тождественные полезным сигналам по структуре и параметрам, но несущие в себе дезинформацию, предназначены для нарушения целостности, искажения, а также изменения алгоритмов передачи-приема и обработки информации [9, 10]. Вследствие создания имитирующих ДВ нарушаются процедуры маршрутизации и определения ранга потребителей информации, возникают перегрузки в каналах информационного обмена для АСУ; для их выявления требуется применять сложные алгоритмы идентификации сигналов, приводящие к задержкам доведения информации.

Современный этап развития ИТС ВДН для обмена данными в АСУ характеризуется следующими тенденциями [12–14]:

использование цифровых, магнитооптических и оптико-электронных технологий формирования и обработки информационных процессов [12, 13];

интеграция процедур передачи-приема и обработки информации в единых устройствах с применением адаптивных мер защиты от непреднамеренных и организованных помех на всех этапах информационного обмена [13, 14].

Таким образом, схемотехнические решения по созданию и функционированию ИТС для АСУ приводят к определению их технического облика в виде пространственно-распределенных структур, базовыми компонентами которых являются средства передачи-приема и обработки

информационных процессов, объединенные линиями (каналами) связи [15–18]. Совместное функционирование компонентов ИТС осуществляется на основе принципов координирования целевых функций и построения единых алгоритмов обработки информации, и доведения до потребителей в соответствии с номенклатурно-временным регламентом [12, 14].

За счет усложнения структуры, правил взаимодействия компонентов [13–18] и увеличения множества функций ИТС ВДН возрастает число элементов, подверженных ДВ [19].

Основными группами элементов, уязвимых в процессе ИПБ, являются:

элементы управления ИТС, позволяющие осуществлять несанкционированные изменения регламента и условий протекания процессов передачи-приема и обработки информации [12, 14, 19];

радиоканалы (радиолинии), по которым возможно поступление команд на несанкционированные изменения алгоритмов информационного обмена и управления компонентами ИТС [13, 14];

устройства передачи-приема и обработки информации с малой степенью защиты; вследствие их интеграции по протоколам взаимодействия и унифицированным форматам информационного обмена в единую информационную платформу реализуются угрозы нарушения нормального состояния ИТС в целом за счет нарушения целостности, полноты и оперативности доведения информации, а также навязывания дезинформации [13, 14, 18–22].

В условиях ИПБ меры по обеспечению безопасности и защиты ИТС от преднамеренных ДВ должны осуществляться при допустимых потерях целевых функций и прогнозируемых изменениях регламента информационного обмена [5, 6, 12, 14].

Сохранение требуемых показателей эффективности передачи-приема и обработки информации при реализации мер по защите достигается за счет создания подсистемы защиты информации (ПЗИ), предназначенной для выявления и нейтрализации компонентов с деструктивными функциями [23], на базе элементов, непосредственно входящих в состав ИТС. Включение ПЗИ в структуру ИТС обеспечивает возможности рационального распределения информационного ресурса, с одной стороны, для выполнения задач целевого предназначения, с другой стороны, для распознавания угроз безопасности информации и адекватного реагирования на них с учетом функциональных взаимосвязей функциональных компонентов и рисков нарушения регламентированных состояний [11, 23, 24].

Цель работы – провести анализ задач и обосновать направления совершенствования защиты ИТС ВДН от преднамеренных ДВ, определить рациональную стратегию функционирования ПЗИ в интересах достижения безопасности информации и информационной инфраструктуры при регламентированных изменениях показателей эффективности информационного обмена.

Актуальность. Защита ИТС ВДН организуется и осуществляется в интересах выполнения следующих основных задач:

снижение эффективности добывания противником данных о состоянии, характеристиках и регламенте функционирования информационной инфраструктуры, а также содержании информации при передаче-приеме и обработке до уровня, не позволяющего создавать преднамеренные ДВ для нарушения режимов информационного обмена [22, 23];

противодействие ДВ путем воспрепятствования их доступу в защищаемые информационные области под видом рабочих компонентов, а также исключения реализации конфликтных компонентов или создания условий их развития с минимизацией ущерба для передаваемой и обрабатываемой информации и информационной инфраструктуры [14, 22].

Защита является эффективной при выполнении требований по надежности сохранения установленных режимов информационного обмена на всех элементах ИТС, подверженных потенциальным угрозам. Рациональная стратегия защиты ИТС характеризуется достижением требуемых показателей эффективности информационного обмена и защищенности информации

СОДЕРЖАНИЕ

и информационной инфраструктуры при всех возможных стратегиях ДВ при ограничениях ресурса, выделяемого для выявления и нейтрализации угроз [3, 7, 12, 14, 23].

Информационная безопасность ИТС ВДН определяется как состояние гарантированной защищенности [24] при выполнении требований по обеспечению информацией потребителей (органов управления, группировок войск, а также отдельных объектов вооружения, военной и специальной техники) [1, 8, 24].

Согласно [14, 21], информационный обмен в условиях ИПБ необходимо рассматривать в рамках информационного конфликта (ИК) компонентов ИТС со средствами ДВ, в котором каждая из сторон стремится достичь максимальной реализации функциональных возможностей при минимизации функций противостоящей стороны. Эффективность ДВ на радиоэлектронные объекты зависит от результатов выполнения задач по добыванию, сбору, обработке информации, обеспечивающей применение средств ИПБ. Поэтому можно утверждать, что конфликтная устойчивость ИТС отражает ее способность выполнить задачу доведения информации с требуемыми показателями эффективности в условиях противодействия [25–27].

В настоящее время в ИТС ВДН защита информации, как правило, осуществляется в соответствии с принципами консервативного реагирования на ДВ [19]:

а) нейтрализация ДВ выполняется путем регламентирования входных и выходных потоков сигналов, контроля целостности и неизменности их параметров, подлежащих идентификации в процессе информационного обмена и контроля безопасности [15];

б) для управления ПЗИ применяются алгоритмы, инвариантные к динамике процесса взаимодействия ИТС со средствами ДВ и ориентированные на нейтрализацию деструктивных компонентов без принятия мер, исключающих повторное проявление аналогичных угроз, а также ДВ с параметрами, адаптированными к изменениям степеней защиты уязвимых объектов [3, 16].

Регламентирование потоков и идентификация характерных признаков сигналов, позволяющие распознать и нейтрализовать ДВ, создаваемые программными средствами несанкционированного доступа в информационные области и постановщиками имитирующих помех ИТС, обеспечивают высокие показатели безопасности отдельных каналов информационного обмена.

Однако фиксация структурных признаков защищаемого элемента не позволяет выявлять вредоносные компоненты, способные маскировать потенциально опасные свойства, изменять свои структурные признаки и корректировать цели воздействия, осуществлять деструктивные функции до полного размещения в среде. Время поиска и нейтрализации таких воздействий, как правило, существенно превышает типовые значения, определяемые из условия достижения требуемого уровня защищенности [14, 17, 28]. Блокировка каналов связи при подавлении маскирующими помехами приводит к распаду целостной структуры ИТС и создает условия для внедрения в информационную среду ДВ, способного выполнить перехват управления и обеспечить нелегитимным абонентам доступ к информации.

Для достижения конфликтной устойчивости ИТС при многократных ДВ, характерных для типовых вариантов ИПБ, необходимо использовать методы активного противодействия угрозам [16, 29]. За счет активного противодействия, в основу которого положены задачи изменения стратегии ДВ по нарушению регламентированных состояний информационного обмена, как показано в [3, 14, 23, 29], достигается нейтрализация угроз безопасности в течение ИК.

На основании изложенного выше можно сделать вывод, что существующая методическая основа обеспечения безопасности и защиты информации с учетом динамики совершенствования средств и способов ДВ не позволяет обеспечить надежное и устойчивое выполнение целевых функций ИТС.

Таким образом, исследования, направленные на повышение конфликтной устойчивости ИТС ВДН в условиях ДВ, носят актуальный характер.

Задачи защиты информационно-телекоммуникационных систем военного и двойного назначения от преднамеренных деструктивных воздействий. Для построения защищенных ИТС ВДН применяются два подхода, разрабатываемых на альтернативной методологической основе [20].

Первый подход базируется на синтезе функциональных блоков системы с объединением в единую структуру за счет установления логико-временных связей в соответствии с целевыми функциями информационного обмена (доведения информации потребителям). В результате создаются наиболее благоприятные условия передачи-приема и обработки информации [23] при требуемых показателях защищенности и безопасности ИТС.

В рамках второго подхода ИТС рассматривается как составная часть системы более высокого уровня, образованной компонентами, входящими в ее состав и состав средств ДВ [3, 29]. Компоненты ИТС, их параметры, цели и задачи, подлежащие выполнению, определяются условиями ИК в соответствии со стратегией функционирования системы более высокого уровня. При этом, в отличие от первого подхода, становится возможным исследование взаимодействия компонентов ИТС не только с компонентами ДВ, но и между собой, в условиях как строгого конфликта (антагонизма), так и содружества (симбиоза) или нейтралитета [18, 21]. Взаимодействие сторон ИПБ по схеме строгого конфликта (антагонизма) рассматривается как противодействие, при котором цели их функционирования прямо противоположны, а изменение целевой функции одной из сторон приводит к строго противоположному (пропорциональному) изменению целевой функции другой стороны. Взаимодействие, принимающее формы содружества (симбиоза), реализует стратегию содействия, при которой целевые функции сторон полностью (частично) совпадают; увеличение эффективности функционирования одной из сторон приводит к строгому (пропорциональному) возрастанию эффективности другой стороны. Нейтралитет представляет собой наименее устойчивую форму взаимодействия, при котором цели взаимодействия компонентов системы высокого уровня могут как совпадать, так и различаться, но изменение эффективности функционирования каждого из них в среднем не влияет на целевые функции других компонентов [21]. В результате становится возможным управление ресурсом системы [16] при рациональных вариантах построения ПЗИ с минимально необходимым временем реакции на ДВ [23].

Перечень основных задач обеспечения безопасности и защиты ИТС ВДН от преднамеренных ДВ включает в себя:

разработку общих алгоритмов управления ПЗИ и элементами ИТС, на которые возложены функции передачи-приема и обработки информации [29], базирующихся на принципах нейтрализации не конкретного ДВ на защищаемые области системы, а непосредственно источника угроз для исключения возможностей их последующего проявления;

создание аппаратно-программных средств из состава ПЗИ с малым временем обнаружения и идентификации ДВ в потоке принимаемых сигналов при минимальном объеме демаскирующих признаков и априорной информации об угрозах активизации конфликтных компонентов [3];

наращивание времени гарантированной стойкости защиты ИТС до значений, определенных требованиями по безопасности информации и информационной инфраструктуры, при неопределенности параметров конфликтующих сторон и дефицитом информационного ресурса, резервируемого для ПЗИ.

Перспективные пути построения ПЗИ определяются по результатам математического (имитационного) моделирования ИК компонентов ИТС и средств ДВ [14, 17]. В имитационных моделях ИТС, подверженных ДВ, воспроизводятся:

а) динамические состояния функциональных компонентов с оценками вероятностно-временных характеристик изменения при угрозах информационной безопасности;

СОДЕРЖАНИЕ

б) процессы (временные параметры процедур) передачи-приема и обработки информации [3, 23, 29] с оценками вероятностно-временных показателей эффективности достижения целевых функций при ДВ.

По результатам анализа реакций компонентов на воздействия и закономерностей изменения регламентированных состояний ИТС [14, 17]:

разрабатываются способы обеспечения требуемой степени безопасности информации и информационной инфраструктуры при регламентированном распределении информационного ресурса на выполнении целевых задач и мероприятий по защите;

формируются рациональный состав и структура; из условий достижения требуемых показателей эффективности информационного обмена и безопасности ИТС определяются алгоритмы совместного функционирования компонентов, задействованных в мероприятиях по защите.

В работах докторов технических наук Борисова В.И., Кузнецова В.И., докторов военных наук Антоновича П.И., Донскова Ю.Е. представлены модели ИТС ВДН, построенные на основе дискретно-событийного представления процессов информационного обмена в условиях ИК со средствами ДВ. Конфликт представляется в виде преднамеренных воздействий на ИТС и реакций их компонентов в целях предотвращения (минимизации) информационного ущерба. При моделировании ИК воспроизводятся состояния компонентов ИТС в дискретные моменты времени и определяются вероятности изменения процессов передачи-приема и обработки информации в целях формирования команд управления в соответствии с целевой функцией информационного обмена [14, 29].

В работах докторов технических наук Владимирова В.И., Сысоева В.В., докторов физико-математических наук Антипова О.И., Неганова В.А. изложены подходы к организации защиты информации и информационной инфраструктуры ИТС ВДН на основе распределения ресурсов, исходя из минимизации потерь целевых функций при опасности угроз, проявляющихся в текущий момент времени.

Однако, как показано в [3, 14, 17, 29], для оценки угроз безопасности информации и информационной инфраструктуре требуется воспроизведение взаимодействия ИТС и ДВ не только на сигнальном, но и семантическом и прагматическом уровнях с учетом взаимосвязей рабочих и конфликтных компонентов сторон [17, 23].

В трудах докторов технических наук Авсентьева О.С., Карташевского В.Г., Павлова В.А., Толстых Н.Н. выполнен синтез и проведена оценка эффективности алгоритмов адаптивного управления структурой и параметрами компонентов ИТС, пребывающих в состояниях конфликта со средствами ДВ, развивающегося по схемам содействия и противодействия [21].

Разработаны следующие адаптивные способы защиты ИТС:

способ пространственно-энергетической адаптации на основе регулирования мощностей передатчиков, чувствительностей приемников и применения приемопередающих антенн с адаптивно изменяемыми показателями пространственно-частотной избирательности передачи-приема сигналов [14, 29];

способ частотно-временной адаптации с применением широкополосных сигналов с множеством несущих частот, псевдослучайной (программной) перестройки рабочих частот передатчиков, передачи сообщений на фоне маскирующих излучений, которые не содержат информации, но затрудняют обработку информационных сигналов средствами мониторинга противостоящей стороны при информационной поддержке процессов создания ДВ [3, 14, 17];

способ структурной адаптации, базирующийся на выборе информационных каналов с минимальными в текущие моменты времени или не выходящими за пределы, определенные требованиями по безопасности, угрозами ДВ [14, 17, 23].

Стратегия адаптивного управления ПЗИ предполагает динамичный перевод ИТС в состояния с минимальными (допустимыми условиями нормального функционирования)

потерями информации за минимальное (регламентированное требованиями к информационному обмену) время по результатам мониторинга угроз безопасности [6, 25].

Вместе с тем, в рамках используемого подхода адаптация ИТС, как правило, выполняется на этапе воспрещения проникновения конфликтного компонента в информационную область. Разрешению подвергаются частные ИК между взаимодействующими компонентами ИТС и ДВ равных уровней иерархии. Варианты адаптации ИТС при реализации конфликтного компонента в информационной области и создания условий его развития с минимальными потерями целевых функций информационного обмена из рассмотрения исключаются ввиду того, что для их реализации на данных этапах требуется значительный объем априорных данных о ДВ, которые в большинстве практически важных случаев не доступны. Взаимодействие компонентов ИТС, адаптируемой к складывающимся условиям, с компонентами ДВ может проявляться на различных уровнях иерархии [28, 31]. Отдельные деструктивные факторы системы способны взаимодействовать с компонентами ИТС не только в форме антагонизма (строгого конфликта), но и на основе содружества (симбиоза) или нейтралитета. Поэтому с применением известных адаптивных способов защиты в общем случае не удается реализовать оптимальную, с позиций обеспечения безопасности информации и информационной инфраструктуры, стратегию ПЗИ при максимально благоприятных условиях достижения целевых функций ИТС [29].

В работах докторов технических наук Герасименко В.А., Калашникова А.О., Куприенко П.С., Новикова Д.А., Поповой Л.Г., Федоркова Е.Д., Язова Ю.К. разработаны модели ситуационного управления сложными объектами и алгоритмы рационального использования информационных ресурсов для противостояния основным классам информационных угроз [32]. Ситуационное управление построено на принципах идентификации текущей ситуации путем сопоставления характерных признаков с вариантами эталонных описаний и последующего выбора типового решения по управлению, наиболее близкого по идентификационному признаку возникающей ситуации [29, 32].

Однако в разработанных моделях воспроизводятся функции и состояния только тех компонентов, которые непосредственно привлекаются для выявления и нейтрализации информационных угроз; имитация работы ИТС в виду необходимости учета большого числа факторов в полной мере затруднена. Это не позволяет привлекать имеющийся в наличии ресурс системы для защиты информации и информационной инфраструктуры, выполнять его рациональное распределение без излишнего снижения эффективности передачи-приема и обработки информации [17, 29].

В работах докторов технических наук Давыдова А.Е., Максимова Р.В., доктора физико-математических наук Потапова А.А. построены модели рефлексивного управления ИТС, суть которого заключается в навязывании противостоящей стороне информации, на основании которой она совершает желаемые действия.

В моделях имитируется комбинаторное взаимодействие пар элементов защищаемых систем и средств ДВ в форме антагонизма (строгого конфликта) с минимизацией выигрыша противостоящей стороны. Алгоритм управления системой рассматривается как процесс формирования состояния, обеспечивающего выполнение ее целевой функции, с учетом стратегии поведения в предыдущие моменты времени, а ДВ, приводящие к изменению состояния ИТС, – как акты управления [15, 21].

Вместе с тем, ввиду иерархической структуры современных ИТС и многоуровневого взаимодействия их компонентов со средствами ДВ, требуется рассматривать варианты матричного (перекрестного) взаимодействия различных элементов конфликтующих сторон на различной основе [12, 24]. Для рационального использования информационных ресурсов каждый из участников ИК должен стремиться максимизировать собственную целевую функцию, не ограничиваясь минимизацией целевой функции противника [17].

Известные модели и методы рефлексивного управления не позволяют синтезировать ПЗИ ИТС без существенной избыточности привлекаемых компонентов; комбинаторная оптимизация структуры и параметров ПЗИ требует значительных вычислительных ресурсов [29, 33].

Общее ограничение возможностей обеспечения безопасности и защиты ИТС на основе адаптивного, ситуационного и рефлексивного управления ее ресурсами заключается в том, что каждый из указанных методов эффективно реализуется только в определенных условиях ДВ и для определенных состояний взаимодействующих элементов. Состояния объектов ДВ изменяются по мере реализации конфликтного компонента в защищаемой структуре, что не позволяет сохранить рациональное соотношение между информационными ресурсами, привлекаемыми для обеспечения безопасности и выполнения целевых функций ИТС на всем интервале времени ИК. В условиях ИК взаимодействие компонентов ИТС и ДВ осуществляется на уровне сложных иерархических систем, в то время как меры защиты обосновываются для вариантов взаимодействия отдельных программно-технических устройств. При этом функции ИК, который необходимо исследовать как конфликт алгоритмов управления организационно-технических структур, реализуются через отдельные элементы ИТС, не затрагивающие их системы управления.

Направления совершенствования защиты информационно-телекоммуникационных систем военного и двойного назначения от преднамеренных деструктивных воздействий. На основании изложенного выше можно утверждать, что в целях определения рационального состава информационных ресурсов для ПЗИ требуется учитывать аспекты многоуровневого и разнопланового взаимодействия ИТС ВДН и ДВ [11, 12, 20].

Модели взаимодействия объектов защиты и средств ДВ должны включать в себя формализованные описания не только компонентов, на которые направлены воздействия, но и самих средств ДВ, что позволит раскрыть их реальные информационные возможности [11, 12]. Поэтому они, во-первых, строятся по иерархическому принципу, во-вторых, воспроизводят функции и состояния структурных элементов на сигнальном, семантическом и прагматическом уровнях [14, 29]. По результатам статистических испытаний таких моделей вырабатываются правила рационального распределения информационного ресурса для функционирования ИТС и выявления и нейтрализации ДВ [23, 29]. Ввиду комплексного характера ДВ на компоненты ИТС конфликт между ними следует рассматривать в рамках концепции системного ИПБ, а разрешение (предотвращение) конфликта – как состояние информационно-временного баланса, определяемого целевыми функциями систем.

Метод управления информационным ресурсом выбирается не из условия наибольшей эффективности нейтрализации угроз безопасности, а по правилу минимизации среднего риска нарушения целевой функции ИТС ВДН. Рациональное управление информационным ресурсом осуществляется путем выбора не только параметров управляющих воздействий, но и методов адаптивного, ситуационного и рефлексивного управления из условия снижения до установленного предела вероятностно-временных характеристик угроз безопасности информации и информационной инфраструктуры системы.

Адаптивное управление защитой ИТС ориентировано на ее перевод в состояние с минимальным средним риском безопасного входа ДВ в защищенную информационную область за счет идентификации компонентов, ориентированных в текущий момент времени на содействие, и мобилизации информационных ресурсов на противодействие непосредственным угрозам.

Эффективность адаптивного управления, оцениваемая по критерию [14, 29] достижения требуемого уровня защиты при допустимых потерях интенсивности информационного обмена, определяется временем изменения структуры и параметров ИТС в складывающейся обстановке [29, 34]. При априори неизвестных целях воздействие осуществляется путем формирования структуры взаимодействующих компонентов в соответствии с целевой функцией выявления и нейтрализации ДВ, а при идентифицированных целях воздействия – путем выбора

СОДЕРЖАНИЕ

рациональных параметров ПЗИ, при которых вероятность реализации целевой функции информационного обмена превышает требуемый уровень.

Ситуационное управление безопасностью и защитой ИТС ВДН [23, 24] осуществляется при ранней идентификации конфликтного взаимодействия ее компонентов со средствами ДВ и базируется на регламентации состояний для преобразования складывающейся ситуации в обобщенную ситуацию с минимальными информационными потерями. Его основу составляет классификация текущего состояния ИТС с целью сведения его к некоторой обобщенной ситуации. Идентификация конфликтного компонента в принятой последовательности унитарных кодов устанавливалась по отличию слов универсальной грамматики на каждом шаге функционирования ИТС [24, 29].

Для анализа эффективности выявления режима конфликтного взаимодействия ИТС ВДН и ДВ определяется вероятность его идентификации при фиксированной вероятности ложной тревоги, определяемой по величине порога принятия решения [24], с последующей оценкой изменения указанных показателей на основе пролонгации [3, 29]. Наибольшая эффективность ситуационного управления достигается за счет нахождения совместной стратегии действий компонентов ИТС, пребывающих в состоянии конфликтного и бесконфликтного взаимодействия.

Рефлексивное управление безопасностью и защитой ИТС ВДН выполняется при проникновении ДВ в информационную область путем имитации рабочих компонентов; оно основано на блокировании их реализации в защищаемой информационной области за счет навязывания действий по минимизации целевых функций вредоносных элементов. При реализации рефлексивного управления выполняется прогноз и оцениваются изменения параметров системы и ДВ в процессе взаимодействия для достижения паритета между ними при возникновении ИК.

Компоненты ИТС и ДВ, обладающие собственными интересами, предпочтениями, при этом выступают в роли активных систем, способных выбирать собственные состояния и корректировать их в складывающейся обстановке, с учетом взаимодействия с другими компонентами [24, 29]. Каждый элемент в соответствие с гипотезой рационального поведения ориентирован на выбор стратегии, при которой его целевая функция достигает максимального значения при информационном равновесии рефлексивной игры компонентов [33].

Эффективность рефлексивного управления определяется не только действиями ПЗИ, но и целевой функцией управляемой системы и системы управления противоборствующей стороны. Наибольшая эффективность управления ПЗИ достигается за счет выбора стратегии поведения, направленной на максимизацию целевых функций ИТС ВДН при одновременной минимизации целевых функций ДВ, при матричном взаимодействии компонентов различных уровней иерархии и комплексном использовании разнородных ресурсов, привлекаемых для защиты [24].

Таким образом, совершенствование защиты ИТС ВДН от ДВ при ИПБ целесообразно проводить по следующим направлениям.

1. Разработка иерархических моделей ИТС ВДН, в которых воспроизводятся ДВ не только на каналы передачи-приема, но и средства обработки информации [29]. Применение моделей позволяет выявить закономерности распределения информационных потоков на объектах информатизации и в телекоммуникационных сетях и рационально распределять информационный ресурс для ПЗИ за счет оптимизации процедур выявления и нейтрализации факторов, оказывающих негативное влияние не только на целевые функции отдельных элементов, но и управление ИТС в целом.

2. Разработка метода адаптивного управления информационным ресурсом ИТС ВДН, который базируется не на переводе систем в состояние с минимальными потерями информации за минимально возможное время при идентификации ДВ [14, 24], а на адаптации компонентов противоборствующих сторон, взаимодействующих на конфликтной и бесконфликтной основе

[29]. В результате оценки состояний элементов ИТС и средств ДВ, способных в текущий момент времени к содействию или нейтралитету [21, 26], обеспечивается рациональное распределение информационного ресурса в соответствии с потребностями защиты.

3. Разработка метода ситуационного управления ИТС ВДН при ДВ, построенного на распознавании конфликтной ситуации и выборе типового решения по управлению компонентами в соответствии с ее эталонным описанием по результатам анализа состояний как противодействующих, так и содействующих компонентов. За счет установления взаимосвязей параметров каждого элемента ИТС с целевой функцией учитывается их вклад в обеспечение безопасности информации, что позволяет осуществлять рациональное управление информационным ресурсом.

4. Разработка метода рефлексивного управления ИТС ВДН при матричном (перекрестном) взаимодействии компонентов защищаемых систем и ДВ в форме конфликта с противоположными целевыми функциями [21]. Стратегия действий каждой из сторон включает не только минимизацию целевой функции оппонента, но и максимизацию собственной целевой функции [29]. Вследствие установления взаимосвязей между элементами ИТС и средств ДВ в состоянии противодействия и содействия достигается сокращение избыточности информационного ресурса, задействованного в ПЗИ [3, 17, 23, 24, 29]; при переходе от анализа комбинаторного взаимодействия компонентов к матричному сокращается время поиска рациональной структуры ПЗИ.

Совершенствование защиты ИТС ВДН по указанным направлениям позволит повысить безопасность информации и информационной инфраструктуры при достижении ее показателей нормативным требованиям [19] и допустимом снижении вероятностно-временных показателей эффективности информационного обмена [35–37]. При этом устанавливается рациональный баланс информационного ресурса для достижения целевой функции передачи-приема и обработки информации, с одной стороны, и реализации мер защиты ИТС от ДВ, с другой стороны [3, 29, 37–40].

Выводы. Проведен анализ задач и направлений совершенствования защиты ИТС ВДН от ДВ. Рассмотрены способы создания ДВ программными средствами несанкционированного доступа в информационные области и комплексами радиоэлектронной борьбы, нарушающими процессы передачи-приема и обработки информации путем постановки маскирующих или имитирующих помех. Исследованы возможности и условия применения методов адаптивного, ситуационного и рефлексивного управления информационным ресурсом защищаемой системы. Показано, что адаптивное управление ПЗИ [14, 23, 24, 29] целесообразно применять при воспрещении проникновения ДВ в защищаемую информационную область ИТС. Методы ситуационного и рефлексивного управления [23, 29] информационным ресурсом ИТВ ВДН наиболее эффективны для нейтрализации ДВ на этапе реализации конфликтных компонентов в информационной области. Ситуационное управление осуществляется путем регламентации состояний ИТС и ДВ для преобразования ситуации их взаимодействия в обобщенную ситуацию с минимальными информационными потерями. Рефлексивное управление базируется на блокировании реализаций конфликтных компонентов в защищаемой информационной области за счет навязывания действий по минимизации целевых функций соответственно.

Определена рациональная стратегия организации защиты в интересах достижения безопасности информации и информационной инфраструктуры при регламентированных изменениях показателей эффективности информационного обмена в информационно-телекоммуникационных системах. Безопасность ИТС ВДН в условиях преднамеренных ДВ при допустимом снижении вероятностно-временных показателей эффективности информационного обмена обеспечивается за счет баланса информационных ресурсов, резервируемых для выполнения задач передачи-приема и обработки информации и реализации целевых функций ПЗИ.

СОДЕРЖАНИЕ

СПИСОК ЛИТЕРАТУРЫ

1. Михайлов Р.Л. Радиоэлектронная борьба в вооруженных силах США. СПб: Наукоемкие технологии, 2018. 131 с.

2. Фененко А.В. Концепция «Быстрого глобального удара» в контексте развития военной стратегии США // Вестник Московского университета. Серия 25: Международные отношения и мировая политика. 2019. № 4. С. 18–50.

3. Жидко Е.А., Разиньков С.Н. Модель подсистемы безопасности и защиты информации системы связи и управления критически важного объекта // Системы управления, связи и безопасности. 2018. № 1. С. 122–135.

4. Михайлов Д.В. Война будущего: возможный порядок нанесения удара средствами воздушного нападения США в многосферной операции на рубеже 2025...2030 годов // Воздушно-космические силы. Теория и практика. 2019. № 12. С. 44–52. [Электронный ресурс]. Режим доступа: http://академия-ввс.рф/images/docs/vks/12-2019/44-52.pdf (дата обращения 15.12.2020).

5. Давыдов А.Е., Максимов Р.В., Савицкий О.К. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. М.: Воентелеком, 2017. 536 с.

6. Малюк А.А. Информационная безопасность. Концептуальные и методологические основы защиты информации. М.: Новое издание, 2003. 386 с.

7. Жидко Е.А. Научно-обоснованный подход к классификации угроз информационной безопасности // Информационные системы и технологии. 2015. № 1 (87). С. 132–139.

8. Ласточкин Ю.И. Роль и место радиоэлектронной борьбы в современных и будущих боевых действиях // Военная мысль. 2015. № 12. С. 12–18.

9. Радиоэлектронная борьба. Тезаурус / под ред. П.А. Созинова. М.: Радиотехника, 2020. 456 с.

10. Кузнецов В.И. Радиосвязь в условиях радиоэлектронной борьбы. Воронеж: ВНИИС, 2002. 403 с.

11. Жидко Е.А., Попова Л.Г. Информационная безопасность: концепция, принципы, методология исследования. Воронеж: ВГАСУ, 2013. 183 с.

12. Жидко Е.А. Высокие интеллектуальные и информационные технологии интегрированного менеджмента XXI века. Воронеж: ВУНЦ ВВС «ВВА», 2014. 76 с.

13. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. СПб.: Наукоемкие технологии, 2017. 546 с.

14. Жидко Е.А., Власов А.Б. Адаптивное управление информационным ресурсом в системе связи критически важного объекта // Инженерно-строительный вестник Прикаспия. 2020. № 3 (33). С. 74–78.

15. Павлов В.А., Пятунин А.Н., Сидоров Ю.В., Толстых Н.Н., Трофимов В.В. Метод оценки эффективности конфликтного функционирования информационной системы // Теория и техника радиосвязи. 2005. № 1. С. 57–62.

16. Толстых Н.Н., Марейченко И.В., Прилуцкий А.М. Модель процесса добывания информации, обрабатываемой в системах управления критических приложений с учетом предыстории их функционирования // Радиолокация, навигация, связь: сб. науч. ст. по материалам X Международной научно-технической конференции (20-22 апреля 2004 г.). Воронеж: ООО НПФ «Саквоее», 2004. Т. 2. С. 1023–1029.

17. Жидко Е.А., Разиньков С.Н. Имитационное моделирование и анализ конфликтного компонента информационно-телекоммуникационной системы с управляемой структурой // Радиолокация, навигация, связь: сб. науч. ст. по материалам XXIV Международной научно-технической конференции (17-19 апреля 2018 г.). Воронеж: ВГУ, 2018. Т. 5. С. 327–334.

18. Кузнецов В.И. Системное проектирование радиосвязи: методы и обеспечение. Воронеж: ВНИИС, 1994. 287 с.

СОДЕРЖАНИЕ

19. Хорошко В.А. Методы и средства защиты информации. М.: Юниор, 2003. 504 с.

20. Жидко Е.А., Попова Л.Г. Формализация программы исследований информационной безопасности компании на основе инноваций // Информация и безопасность. 2012. Т. 15. № 4. С. 471–478.

21. Владимиров В.И. Принципы и аппарат системных исследований радиоэлектронного конфликта. Воронеж: ВВВИУРЭ, 1992. 107 с.

22. Жидко Е.А., Попова Л.Г. Принципы системного математического моделирования информационной безопасности // Науковедение. 2014. № 2 (21). С. 34–39.

23. Жидко Е.А., Разиньков С.Н. Организация подсистемы безопасности и защиты информации экологически опасного критически важного объекта // Вестник Воронежского института ГПС МЧС России. 2018. № 1 (26). С. 59–63.

24. Жидко Е.А., Разиньков С.Н. Стратегии управления безопасностью информации в информационно-телекоммуникационных системах // Информатика: проблемы, методология, технологии: сб. науч. ст. по материалам XIX Международной научной конференции (15-16 февраля 2019 г.). Воронеж: ВГУ, 2019. Т. 2. С. 389–397.

25. Меньшаков Ю.К. Теоретические основы технических разведок. М.: МГТУ имени Н.Э. Баумана, 2008. 536 с.

26. Владимиров В.И., Владимиров И.В., Наметкин В.В. Избранные вопросы радиоэлектронного подавления цифровых каналов систем радиосвязи. Воронеж: ВАИУ, 2010. 119 с.

27. Владимиров В.И., Владимиров И.В., Наметкин В.В. Информационные основы радиоэлектронного подавления цифровых каналов передачи информации систем радиосвязи. Воронеж: ВУНЦ ВВС «ВВА», 2015. 296 с.

28. Толстых Н.Н., Марейченко И.В., Буянов С.В. Модель адаптивной системы защиты информации. Управление безопасностью // Теория и техника радиосвязи. 2004. № 2. С. 32–34.

29. Кочкаров А.А., Разиньков С.Н., Тимошенко А.В., Шевцов В.А. Комплексный метод управления информационными ресурсами безопасности телекоммуникационных систем авиационных комплексов мониторинга // Известия вузов. Авиационная техника. 2020. № 2. С. 158–166.

30. Лукацкий А.В. Адаптивное управление защитой // Сети. Глобальные сети и телекоммуникации. 1999. № 10. С. 89–95.

31. Жданов А.А. Метод автономного адаптивного управления и его приложения // Прикладные информационные технологии и интеллектуальные системы. 2004. № 6. С. 56–61.

32. Поспелов Д.А. Принципы ситуационного управления // Известия АН СССР. Техническая кибернетика. 1971. № 2. С. 435–441.

33. Новиков Д.А., Чхартишвили А.Г. Рефлексивные игры. М.: СИНТЕГ, 2003. 149 с.

34. Максимов Р.В., Павловский А.В., Стародубцев Ю.И. Защита информации от технических средств разведки в системах связи и автоматизации. СПб.: ВАС, 2007. 88 с.

35. Kochkarov A.A., Razinkov S.N., Timoshenko A.V., Shevtsov V.A. Comprehensive method of information resources control ensuring the security of telecommunication system of aviation monitoring complex // Russian Aeronautics. 2020. Vol. 63. № 2. P. 347–356. DOI: 10.103/S1068799820020233.

36. Разиньков С.Н. Основные направления развития и базовые технологии создания систем радиосвязи со сверхширокополосными сигналами // Воздушно-космические силы. Теория и практика. 2019. № 11. С. 38–43. [Электронный ресурс]. Режим доступа: http://академия-ввс.рф/images/docs/vks/11-2019/38-43.pdf (дата обращения 15.12.2020).

37. Попова С.В., Федоринов В.Е. Экономические аспекты информационной безопасности // Воздушно-космические силы. Теория и практика. 2018. № 5. С. 17–24. [Электронный ресурс]. Режим доступа: http://академия-ввс.рф/images/data/zhurnal_vks/5-2018/17-24.pdf (дата обращения 15.12.2020).

СОДЕРЖАНИЕ

38. Полунин Е.С. Проблема информационной безопасности государства в современных научных исследованиях // Воздушно-космические силы. Теория и практика. 2018. № 7. С. 43–54. [Электронный ресурс]. Режим доступа: http://академия-ввс.рф/images/data/zhurnal_vks/7-2018/43-54.pdf (дата обращения 15.12.2020).

39. Жидко Е.А., Попова Л.Г. Логико-вероятностно-информационное моделирование информационной безопасности // Вестник Казанского государственного технического университета имени А.Н. Туполева. 2014. № 4. С. 136–140.

40. Жидко Е.А., Разиньков С.Н. Способы управления защитой информационно-телекоммуникационной системы // Физика и технические приложения волновых процессов: сб. науч. ст. по материалам XVI Международной научно-хнической конференции (17-21 сентября 2018 г.). Миасс: ЮУГУ, 2019. Т. 2. С. 33–34.

REFERENCES

1. Mihajlov R.L. Radio`elektronnaya bor'ba v vooruzhennyh silah SShA. SPb: Naukoemkie tehnologii, 2018. 131 p.

2. Fenenko A.V. Koncepciya «Bystrogo global'nogo udara» v kontekste razvitiya voennoj strategii SShA // Vestnik Moskovskogo universiteta. Seriya 25: Mezhdunarodnye otnosheniya i mirovaya politika. 2019. № 4. pp. 18–50.

3. Zhidko E.A., Razin'kov S.N. Model' podsistemy bezopasnosti i zaschity informacii sistemy svyazi i upravleniya kriticheski vazhnogo ob`ekta // Sistemy upravleniya, svyazi i bezopasnosti. 2018. № 1. pp. 122–135.

4. Mihajlov D.V. Vojna buduschego: vozmozhnyj poryadok naneseniya udara sredstvami vozdushnogo napadeniya SShA v mnogosfernoj operacii na rubezhe 2025...2030 godov // Vozdushno-kosmicheskie sily. Teoriya i praktika. 2019. № 12. pp. 44–52. [`Elektronnyj resurs]. Rezhim dostupa: http://akademiya-vvs.rf/images/docs/vks/12-2019/44-52.pdf (data obrascheniya 15.12.2020).

5. Davydov A.E., Maksimov R.V., Savickij O.K. Zaschita i bezopasnost' vedomstvennyh integrirovannyh infokommunikacionnyh sistem. M.: Voentelekom, 2017. 536 p.

6. Malyuk A.A. Informacionnaya bezopasnost'. Konceptual'nye i metodologicheskie osnovy zaschity informacii. M.: Novoe izdanie, 2003. 386 p.

7. Zhidko E.A. Nauchno-obosnovannyj podhod k klassifikacii ugroz informacionnoj bezopasnosti // Informacionnye sistemy i tehnologii. 2015. № 1 (87). pp. 132–139.

8. Lastochkin Yu.I. Rol' i mesto radio`elektronnoj bor'by v sovremennyh i buduschih boevyh dejstviyah // Voennaya mysl'. 2015. № 12. pp. 12–18.

9. Radio`elektronnaya bor'ba. Tezaurus / pod red. P.A. Sozinova. M.: Radiotehnika, 2020. 456 p.

10. Kuznecov V.I. Radiosvyaz' v usloviyah radio`elektronnoj bor'by. Voronezh: VNIIS, 2002. 403 p.

11. Zhidko E.A., Popova L.G. Informacionnaya bezopasnost': koncepciya, principy, metodologiya issledovaniya. Voronezh: VGASU, 2013. 183 p.

12. Zhidko E.A. Vysokie intellektual'nye i informacionnye tehnologii integrirovannogo menedzhmenta XXI veka. Voronezh: VUNC VVS «VVA», 2014. 76 p.

13. Makarenko S.I. Informacionnoe protivoborstvo i radio`elektronnaya bor'ba v setecentricheskih vojnah nachala XXI veka. SPb.: Naukoemkie tehnologii, 2017. 546 p.

14. Zhidko E.A., Vlasov A.B. Adaptivnoe upravlenie informacionnym resursom v sisteme svyazi kriticheski vazhnogo ob`ekta // Inzhenerno-stroitel'nyj vestnik Prikaspiya. 2020. № 3 (33). pp. 74–78.

15. Pavlov V.A., Pyatunin A.N., Sidorov Yu.V., Tolstyh N.N., Trofimov V.V. Metod ocenki `effektivnosti konfliktnogo funkcionirovaniya informacionnoj sistemy // Teoriya i tehnika radiosvyazi. 2005. № 1. pp. 57–62.

СОДЕРЖАНИЕ

16. Tolstyh N.N., Marejchenko I.V., Priluckij A.M. Model' processa dobyvaniya informacii, obrabatyvaemoj v sistemah upravleniya kriticheskih prilozhenij s uchetom predystorii ih funkcionirovaniya // Radiolokaciya, navigaciya, svyaz': sb. nauch. st. po materialam X Mezhdunarodnoj nauchno-tehnicheskoj konferencii (20-22 aprelya 2004 g.). Voronezh: OOO NPF «Sakvoee», 2004. T. 2. pp. 1023–1029.

17. Zhidko E.A., Razin'kov S.N. Imitacionnoe modelirovanie i analiz konfliktnogo komponenta informacionno-telekommunikacionnoj sistemy s upravlyaemoj strukturoj // Radiolokaciya, navigaciya, svyaz': sb. nauch. st. po materialam XXIV Mezhdunarodnoj nauchno-tehnicheskoj konferencii (17-19 aprelya 2018 g.). Voronezh: VGU, 2018. T. 5. pp. 327–334.

18. Kuznecov V.I. Sistemnoe proektirovanie radiosvyazi: metody i obespechenie. Voronezh: VNIIS, 1994. 287 p.

19. Horoshko V.A. Metody i sredstva zaschity informacii. M.: Yunior, 2003. 504 p.

20. Zhidko E.A., Popova L.G. Formalizaciya programmy issledovanij informacionnoj bezopasnosti kompanii na osnove innovacij // Informaciya i bezopasnost'. 2012. T. 15. № 4. pp. 471–478.

21. Vladimirov V.I. Principy i apparat sistemnyh issledovanij radio`elektronnogo konflikta. Voronezh: VVVIUR`E, 1992. 107 p.

22. Zhidko E.A., Popova L.G. Principy sistemnogo matematicheskogo modelirovaniya informacionnoj bezopasnosti // Naukovedenie. 2014. № 2 (21). pp. 34–39.

23. Zhidko E.A., Razin'kov S.N. Organizaciya podsistemy bezopasnosti i zaschity informacii `ekologicheski opasnogo kriticheski vazhnogo ob`ekta // Vestnik Voronezhskogo instituta GPS MChS Rossii. 2018. № 1 (26). pp. 59–63.

24. Zhidko E.A., Razin'kov S.N. Strategii upravleniya bezopasnost'yu informacii v informacionno-telekommunikacionnyh sistemah // Informatika: problemy, metodologiya, tehnologii: sb. nauch. st. po materialam XIX Mezhdunarodnoj nauchnoj konferencii (15-16 fevralya 2019 g.). Voronezh: VGU, 2019. T. 2. pp. 389–397.

25. Men'shakov Yu.K. Teoreticheskie osnovy tehnicheskih razvedok. M.: MGTU imeni N.`E. Baumana, 2008. 536 p.

26. Vladimirov V.I., Vladimirov I.V., Nametkin V.V. Izbrannye voprosy radio`elektronnogo podavleniya cifrovyh kanalov sistem radiosvyazi. Voronezh: VAIU, 2010. 119 p.

27. Vladimirov V.I., Vladimirov I.V., Nametkin V.V. Informacionnye osnovy radio`elektronnogo podavleniya cifrovyh kanalov peredachi informacii sistem radiosvyazi. Voronezh: VUNC VVS «VVA», 2015. 296 p.

28. Tolstyh N.N., Marejchenko I.V., Buyanov S.V. Model' adaptivnoj sistemy zaschity informacii. Upravlenie bezopasnost'yu // Teoriya i tehnika radiosvyazi. 2004. № 2. pp. 32–34.

29. Kochkarov A.A., Razin'kov S.N., Timoshenko A.V., Shevcov V.A. Kompleksnyj metod upravleniya informacionnymi resursami bezopasnosti telekommunikacionnyh sistem aviacionnyh kompleksov monitoringa // Izvestiya vuzov. Aviacionnaya tehnika. 2020. № 2. pp. 158–166.

30. Lukackij A.V. Adaptivnoe upravlenie zaschitoj // Seti. Global'nye seti i telekommunikacii. 1999. № 10. pp. 89–95.

31. Zhdanov A.A. Metod avtonomnogo adaptivnogo upravleniya i ego prilozheniya // Prikladnye informacionnye tehnologii i intellektual'nye sistemy. 2004. № 6. pp. 56–61.

32. Pospelov D.A. Principy situacionnogo upravleniya // Izvestiya AN SSSR. Tehnicheskaya kibernetika. 1971. № 2. pp. 435–441.

33. Novikov D.A., Chhartishvili A.G. Refleksivnye igry. M.: SINTEG, 2003. 149 p.

34. Maksimov R.V., Pavlovskij A.V., Starodubcev Yu.I. Zaschita informacii ot tehnicheskih sredstv razvedki v sistemah svyazi i avtomatizacii. SPb.: VAS, 2007. 88 p.

35. Kochkarov A.A., Razinkov S.N., Timoshenko A.V., Shevtsov V.A. Comprehensive method of information resources control ensuring the security of telecommunication system of aviation

СОДЕРЖАНИЕ

monitoring complex // Russian Aeronautics. 2020. Vol. 63. № 2. pp. 347–356. DOI: 10.103/S1068799820020233.

36. Razin'kov S.N. Osnovnye napravleniya razvitiya i bazovye tehnologii sozdaniya sistem radiosvyazi so sverhshirokopolosnymi signalami // Vozdushno-kosmicheskie sily. Teoriya i praktika. 2019. № 11. pp. 38–43. [`Elektronnyj resurs]. Rezhim dostupa: http://akademiya-vvs.rf/images/docs/vks/11-2019/38-43.pdf (data obrascheniya 15.12.2020).

37. Popova S.V., Fedorinov V.E. `Ekonomicheskie aspekty informacionnoj bezopasnosti // Vozdushno-kosmicheskie sily. Teoriya i praktika. 2018. № 5. pp. 17–24. [`Elektronnyj resurs]. Rezhim dostupa: http://akademiya-vvs.rf/images/data/zhurnal_vks/5-2018/17-24.pdf (data obrascheniya 15.12.2020).

38. Polunin E.S. Problema informacionnoj bezopasnosti gosudarstva v sovremennyh nauchnyh issledovaniyah // Vozdushno-kosmicheskie sily. Teoriya i praktika. 2018. № 7. pp. 43–54. [`Elektronnyj resurs]. Rezhim dostupa: http://akademiya-vvs.rf/images/data/ zhurnal_vks/7-2018/43-54.pdf (data obrascheniya 15.12.2020).

39. Zhidko E.A., Popova L.G. Logiko-veroyatnostno-informacionnoe modelirovanie informacionnoj bezopasnosti // Vestnik Kazanskogo gosudarstvennogo tehnicheskogo universiteta imeni A.N. Tupoleva. 2014. № 4. pp. 136–140.

40. Zhidko E.A., Razin'kov S.N. Sposoby upravleniya zaschitoj informacionno-telekommunikacionnoj sistemy // Fizika i tehnicheskie prilozheniya volnovyh processov: sb. nauch. st. po materialam XVI Mezhdunarodnoj nauchno-hnicheskoj konferencii (17-21 sentyabrya 2018 g.). Miass: YuUGU, 2019. T. 2. pp. 33–34.

Жидко Елена Александровна, доктор технических наук, доцент, профессор кафедры техносферной и пожарной безопасности, Воронежский государственный технический университет, Россия, 394006, г. Воронеж, ул. 20-летия Октября, 84, lenag66@mail.ru.

Кущев Сергей Сергеевич, кандидат технических наук, доцент, начальник кафедры автоматизированных систем управления и информационной безопасности, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж), Россия, 394064, г. Воронеж, ул. Старых Большевиков, 54А, serkser@list.ru.

Разиньков Сергей Николаевич, доктор физико-математических наук, старший научный сотрудник, ведущий научный сотрудник Научно-исследовательского испытательного института (радиоэлектронной борьбы), Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж), Россия, 394064, г. Воронеж, ул. Старых Большевиков, 54А, razinkovsergey@rambler.ru.

Тенячкин Сергей Владимирович, старший помощник начальника отдела учебно-методического центра, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж), Россия, 394064, г. Воронеж, ул. Старых Большевиков, 54А.

СОДЕРЖАНИЕ