УДК: 007

СПОСОБ СОЗДАНИЯ РЕЗЕРВНОЙ КОПИИ СЛОЖНОГО ОБЪЕКТА

METHOD FOR BACKING UP COMPLEX OBJECT STATE

Д-р воен. наук Ю.И. Стародубцев, канд. техн. наук С.А. Иванов,
канд. техн. наук П.В. Закалкин, канд. техн. наук Е.В. Вершенник

D.Sc. J.I. Starodubcev, Ph.D. S.A. Ivanov, Ph.D. P.V. Zakalkin, Ph.D. E.V. Vershennik

ВАС им. С.М. Буденного

Сложные технологические системы, использующие ресурсы киберпространства, подвергаются множеству скоординированных воздействий на них как организованных хакерских сообществ, так и кибертеррористов. Частично воздействия направлены на перевод сложных технологических систем в критические (закритические) режимы функционирования за счет изменения условий и параметров функционирования объекта. Это обуславливает необходимость создания резервных копий сложного объекта для его последующего оперативного восстановления. Существующие подходы к созданию резервных копий сложного объекта требуют больших вычислительных мощностей, хранилищ данных и временных затрат, что негативно влияет на работу системы. В статье рассматривается способ создания резервной копии сложного объекта. Предлагаемый способ позволяет снизить затраты ресурсов вычислительной мощности, оперативной памяти, хранилища данных и времени на создание резервной копии состояния сложного объекта.
Ключевые слова: сложный объект, резервная копия.

Complex technological systems that use the resources of cyberspace are subjected to a variety of coordinated impacts on them by both organized hacker communities and cyberterrorists. In part, the impacts are aimed at transferring complex technological systems to critical (off-critical) modes of operation, due to changes in the conditions and parameters of the operation of the object. This makes it necessary to create backups of a complex object, for its subsequent operational recovery. Existing approaches to creating backups of a complex object require a lot of computing power, data storage, and time, which negatively affects the operation of the system. This article discusses how to create a backup copy of a complex object. The proposed method allows you to reduce the cost of computing power, RAM, data storage, and time to create a backup copy of the state of a complex object.
Keywords: a complex object, the backup copy.

Являясь сложным высокотехнологичным объектом, киберпространство интегрировало в себя множество технологических процессов. Посредством киберпространства осуществляется управление технологическими процессами, реализованными в рамках объектов и субъектов критической инфраструктуры государства, в том числе банковской системой, логистическими процессами, энергетикой, водоснабжением, медициной, образованием и др. Таким образом, множество сложных программно-аппаратных объектов вынуждено функционировать с использованием ресурсов киберпространства [1–3].

При этом воздействия посредством киберпространства могут быть осуществлены не только непосредственно на целевой сложный объект, но и на технологические системы, обеспечивающие его функционирование, такие как сети операторов связи, автоматизированные системы управления технологическими процессами и т.д. Результатом таких воздействий является перевод сложного объекта в режим некорректного функционирования или критическое состояние [4–7].

Существование критических состояний обусловлено следующими причинами: наличием ошибок при проектировании и конструировании объекта; большой неопределенностью (непредсказуемостью) состояний в связи с высокой сложностью объекта; недостаточностью необходимого ресурса для устранения известных критических состояний, в том числе и отсутствием соответствующих технологий.

В случае перехода сложного объекта в некорректное состояние необходимо его восстановление до первоначальных (корректных) параметров, для чего, как правило, используется предварительно созданная резервная копия.

В настоящее время существуют следующие подходы к созданию резервных копий сложных объектов. В первом случае, периодически создаются полные копии программной составляющей объекта, во втором — создается полная копия первоначального состояния, а затем периодически записывают только изменения, произошедшие после полного копирования.

Реализация первого подхода для сложного объекта требует больших затрат ресурсов вычислительной мощности, оперативной памяти, хранилища данных и времени, что создает большую нагрузку на каналы передачи данных при удаленном копировании состояния объекта или его элементов.

Второй подход требует меньших ресурсов для создания резервных копий и создает гораздо меньшую нагрузку на каналы передачи данных при удаленном копировании. Однако процесс восстановления объектов занимает существенно больше времени, что может быть критичным для их целевого функционирования.

Кроме того, проблематичность резервного копирования программной составляющей сложных объектов обусловлена рядом взаимоувязанных факторов, к которым относятся:

– возможная территориальная рассредоточенность элементов;

– наличие одной и более автоматизированных систем управления различных элементов;

– необходимость создания актуальных работоспособных резервных копий всех функций и элементов;

– экспоненциальный рост сложности систем автоматизации контроля, резервного копирования и восстановления объекта с ростом количества его элементов и функций;

– существенная разница требований к качеству, контролю и восстановлению различных функций объекта;

– сложные взаимозависимости между функциями, элементами, показателями функций и элементов.

Известные подходы [8–10] в области резервного копирования состояния сложного объекта обладают следующими основными недостатками:

– высокая нагрузка на ресурсы многопараметрического объекта, затрачиваемые на его резервное копирование (вычислительной мощности, оперативной памяти, хранилища данных и времени);

– усложнение средств автоматизации управления резервным копированием объекта в условиях современных тенденций увеличения сложности программно-аппаратных объектов.

Таким образом, задача снижения затрат ресурсов вычислительной мощности, оперативной памяти, хранилища данных и времени на создание резервной копии состояния сложного объекта является актуальной. Решение данной задачи предлагается в разработанном способе резервного копирования состояния сложного объекта [11]. Обобщенная структурно-логическая последовательность действий предлагаемого способа представлена на рис. 1.

На первоначальном этапе осуществляют настройку сложного объекта в соответствии с исходными данными и создают резервную копию его функций.

В качестве исходных данных задают:

– множество M элементов сложного объекта. Например, в состав сети связи входят сервера, конверторы, агрегаторы, коммутаторы, маршрутизаторы, мулитиплексоры и др., различных технологоий и производителей;

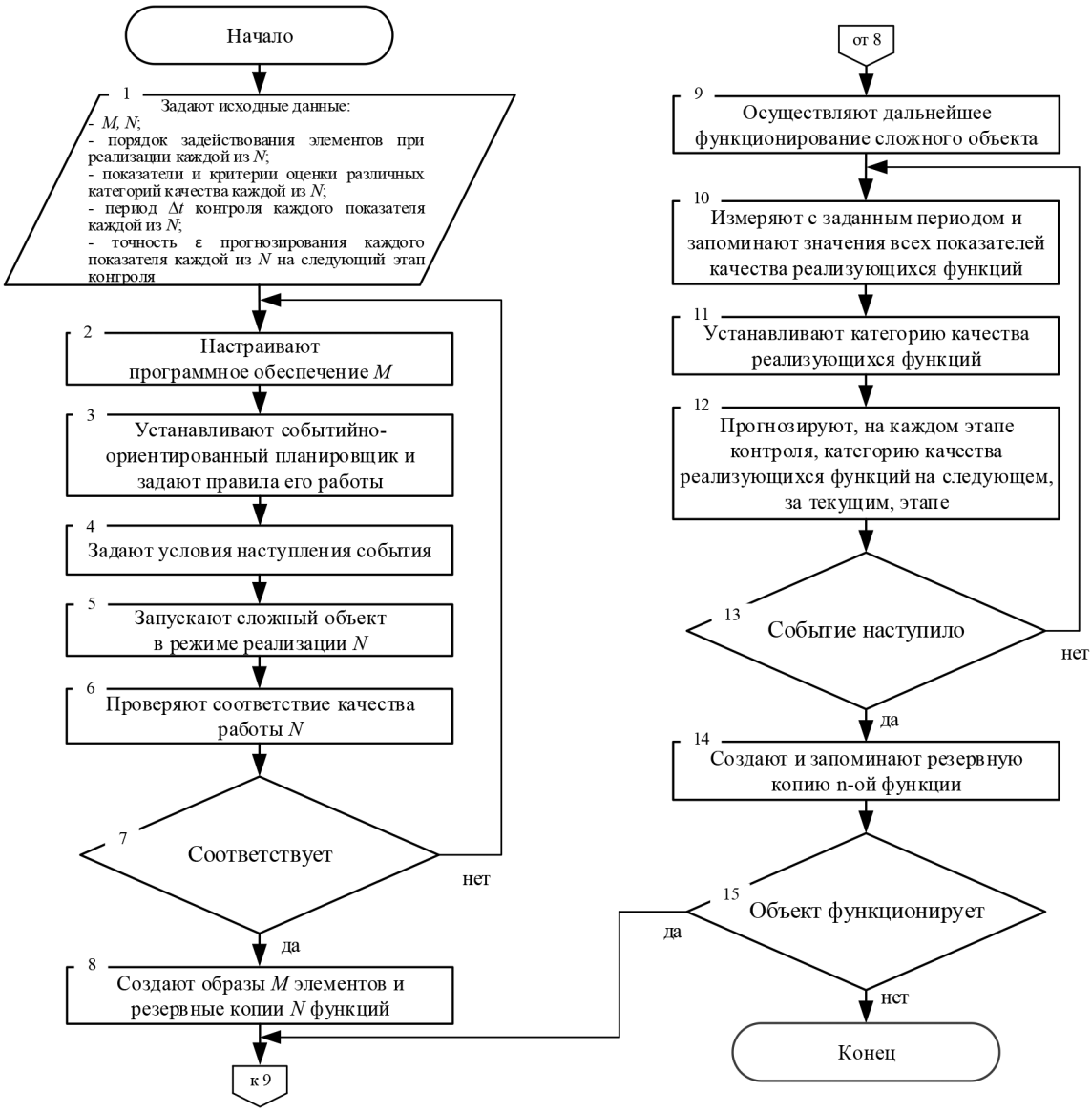

Рис. 1. Обобщенная структурно-логическая последовательность действий способа копирования состояния сложного объекта

– множество N функций сложного объекта. Например, в мультисервисных сетях связи могут быть реализованы следующие функции: передачи речи, данных, видео, телеметрии; синхронизации, резервирования, информационной безопасности, гарантированного энергообеспечения и т.д.;

– порядок задействования элементов сложного объекта при реализации каждой функции (рис. 2). В реализации отдельной функции сложного объекта могут быть задействованы один и более элементов (M_n), рассредоточенных на местности (например, транспортная сеть связи) или сосредоточенных на одном физическом объекте.

В приведенной схеме (рис. 2) различные штриховые линии соответствуют отдельным функциям сложного объекта. Так при реализации функции N_1 сложного объекта задействуются элементы M_1, M_2, M_i и далее, согласно заданного порядка, до элемента M_m. В реализации отдельной функции сложного объекта могут быть задействованы один и более элементов, рассредоточенных на местности (например, транспортная сеть связи) или сосредоточенных на одном физическом объекте (например, вертолет). Функция может реализоваться однотипными (маршрутизаторы, при передаче трафика

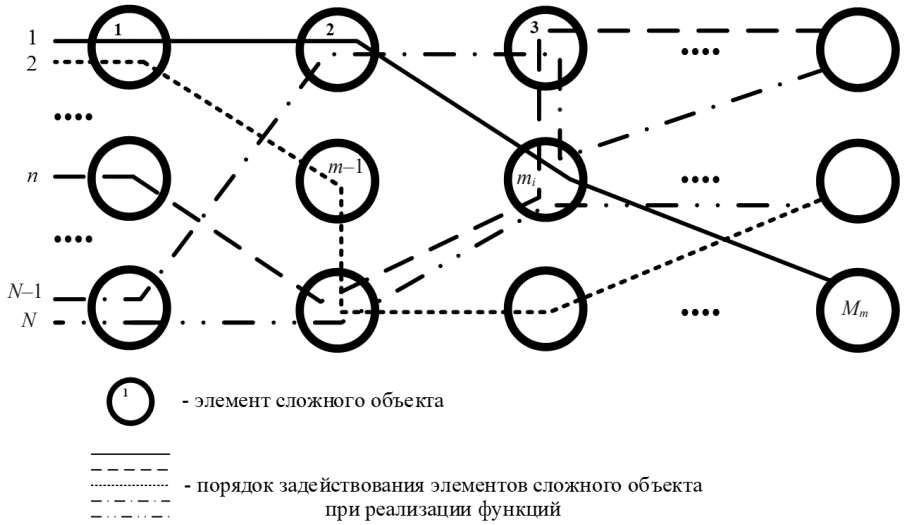

Рис. 2. Графическое отображение порядка задействования элементов сложного объекта при реализации его функций

в транспортной сети), разнотипными (фильтр, насос, топливная магистраль, форсунка, при подаче топлива в сопло реактивного двигателя), либо комбинированным применением нескольких разнотипных элементов (компьютеры, коммутаторы, сервера различного назначения, сеть электропитания при обмене данными в локальной вычислительной сети);

– показатели и критерии оценки различных категорий качества для каждой функции. Задание показателей и критериев оценки различных категорий качества функций сложного объекта возможно исходя из результатов его моделирования, проектирования и производства. Значения показателей функции сложного объекта определяют качество ее реализации, при этом не все показатели подлежат обязательному контролю. Для определения качества функции достаточно контролировать перечень максимально информативных, базовых показателей (показателей качества), на основе которых, за счет установленных взаимозависимостей между показателями функции, возможно вычислить остальные показатели функции, что позволит снизить нагрузку на средства контроля и автоматизации управления сложного объекта (например: сложный объект — сеть связи; функция — устойчивость; показатели — коэффициент готовности, коэффициент оперативной готовности, время ремонта и др.; критерии оценки определяются в соответствии с категорией сети связи) [12];

– предельные значения показателей качества для каждой функции N, задаваемые в соответствии с установленными для данной функции требованиями. Выход показателя за предельные значения может иметь различные последствия — от срыва плановых мероприятий и финансовых потерь (например — нарушение работы биллинга оператора связи), до выхода из строя элементов, либо критического разрушения объекта, который она обслуживает (например — автоматизированные системы управления критической инфраструктурой). Поэтому резервная копия функций сложного объекта должна создаваться до выхода их показателей качества за предельные значения, а введение градации категорий качества показателей функций позволит своевременно, последовательно и обоснованно прогнозировать их тенденции к возможному выходу за предельные значения и обоснованно предпринимать соответствующие действия;

– период контроля каждого показателя каждой из N функций; для каждого показателя N-ой функции может задаваться на наихудший случай [13, 14], либо оптимизироваться в соответствии с интенсивностью изменения показателя в текущем периоде работы функции;

– точность прогнозирования каждого показателя N функций на следующий, за текущим, этапе контроля. Степень сходства заявленных (прогнозируемых) значений показателей с реальными для каждого показателя N функций задается отдельно, в том числе, если различные

функции оцениваются одинаковыми показателями. Это обусловлено сложными взаимосвязями функций и их показателей внутри объекта, а также различиями требований к функциям — к одному показателю отдельного элемента могут предъявляться различные требования (критерии) в отношении различных функций.

Заданные исходные данные заносят в запоминающие устройства (ЗУ) автоматизированной системы управления сложным объектом.

После этого, настраивают программное обеспечение *M* элементов сложного объекта в соответствии с исходными данными. Один элемент сложного объекта может использоваться при реализации одной и более функций, поэтому необходимо проводить настройку элементов сложного объекта согласно полных перечней функций, в реализации которых они могут участвовать. Как правило, сложные объекты индивидуальны, либо мелкосерийны, поэтому для них разрабатывается специализированное программное обеспечение, либо индивидуальные надстройки и настройки серийного программного обеспечения. Такое программное обеспечение требует индивидуальной доработки и настройки, а также возможности «ручного» управления.

Для реализации функции создания резервных копий реализующихся функций сложного объекта в соответствии с заданными правилами его работы в виде наступления событий устанавливают событийно-ориентированный планировщик.

Для этого задают условие наступления события (блок 4, рис. 1) в случае, если результат прогноза любого показателя качества *n*-ой функции выходит за предельные значения качества. На этом этапе необходимо задать полное множество показателей качества *N* функций сложного объекта, подлежащих контролю, и их предельные значения в соответствии с установленными, либо известными взаимосвязями показателей между собой.

В блоке 5 запускают сложный объект в режиме реализации всех функций и в блоках 12, 13 проверяют соответствие качества работы *N* функций сложного объекта заданным требованиям. Если качество работы функций не удовлетворяет требованиям, то проводят коррекцию настроек программного обеспечения элементов сложного объекта до тех пор, пока все функции не будут работать корректно. На данном этапе не рассматривается неисправность аппаратной части элементов сложного объекта, поскольку это должно быть проверено на этапе их разработки и производства (научно-исследовательских и опытно-конструкторских работ, приемки составных элементов представителями заказчика). Все вопросы аппаратной надежности в режиме полной нагрузки сложного объекта должны быть учтены на этапах, предшествующих вводу объекта в эксплуатацию.

Если качество работы функций удовлетворяет требованиям, то создают резервную копию каждой из *N* функций сложного объекта (блок 8, рис. 2), состоящую из образов реализующих ее элементов. Образы элементов записывают в ЗУ автоматизированной системы управления сложным объектом, карты реализации функций (обозначения элементов сложного объекта и порядок их взаимодействия при реализации каждой из *N* функций) заносятся в базу данных.

После этого осуществляют дальнейшее функционирование сложного объекта в штатном режиме. Как правило, сложным объектам не свойственно работать в режиме реализации всех функций (например, при запуске ракеты силовые установки различных ступеней работают поочередно, а их одновременное применение недопустимо). Поэтому показатели качества реализуемых функций измеряют с заданным периодом и запоминают значения всех показателей качества, только реализующихся функций сложного объекта. Это снижает нагрузку на ресурсы системы контроля (вычислительной мощности, оперативной памяти, хранилища данных и времени) состояния сложного объекта.

Для измерения могут использоваться как отдельные устройства, так и измерительные комплексы. Так, для волоконно-оптической системы передачи используются: рефлектометр для измерения характеристик линейного тракта (оптического волокна), когерентные измерители рассеянных сигналов для поиска виброакустических (деструктивных) воздействий на оптический кабель и повреждений, микроскоп для определения качества торцов оптического волокна, измерители оптической мощности для определения параметров сигнала, анализаторы транспортных сетей для тестирования канального оборудования и т.д.

В блоке 11 устанавливают категорию качества для всех показателей качества реализу-

ющихся функций в соответствии с заданными критериальными значениями различных категорий качества путем сравнения заданных критериальных значений различных категорий качества реализующихся функций с результатами измерений. Результаты записывают в ПЗУ автоматизированной системы управления сложным объектом.

После этого с заданной точностью ε прогнозируют, на каждом этапе контроля показателей, категорию качества показателей качества реализующихся функций на следующем, за текущим этапе контроля. Для выполнения требований к точности прогнозирования необходимо набрать статистические данные, объем которых позволит выполнить требования к прогнозированию на установленном промежутке времени. Для этого сложный объект должен функционировать достаточный период времени для набора необходимого объема статистических данных о всех показателях качества N функций. Данный период должен входить в этап пусконаладочных мероприятий. Учитывая то, что способ предполагает прогнозирование значений параметров только на следующей, за текущим этапом контроля, то точность прогнозирования при соответствующем объеме статистики, в отсутствии непредусмотренных при разработке сложного объекта деструктивных факторов, будет высокой. Результаты прогнозирования записывают в ЗУ автоматизированной системы управления сложным объектом.

На каждом этапе контроля устанавливают категорию качества показателей качества реализующихся функций путем сравнения заданных критериальных значений различных категорий качества функций с результатами прогнозирования на следующий этап контроля. Если результат прогноза любого показателя n-ой функции выходит за предельные значения качества, то событийно-ориентированный планировщик фиксирует событие по n-ой функции.

При наступлении события создают резервную копию n-ой функции сложного объекта, путем создания образов, реализующих ее M_n элементов. Образы элементов записывают в ЗУ автоматизированной системы управления сложным объектом, карты реализации функций (обозначения элементов сложного объекта и порядок их взаимодействия при реализации каждой из N функций) заносят в ее базу данных для восстановления n-ой функции сложного объекта при выполнении прогноза выхода ее параметров за предельные значения.

Выводы

Представленный в статье способ обеспечивает создание резервных копий состояния сложного объекта на протяжении всего его времени функционирования. Таким образом, за счет копирования состояния сложного объекта по функциям при их прогнозируемом выходе за предельные значения показателей качества, а также введения категорий показателей качества, позволяющих последовательно и обоснованно прогнозировать выход функций за предельные значения показателей качества, снижаются затраты ресурсов вычислительной мощности, оперативной памяти, хранилища данных и времени на создание резервной копии состояния сложного объекта. Научная новизна и практическая значимость предлагаемого способа подтверждается патентом на изобретение [12].

Литература

1. Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Проблемы функционирования сложных систем, использующих ресурсы киберпространства // В сборнике: Радиолокация, навигация, связь. Сборник трудов XXVI Международной научно-технической конференции, в 6 т. — Воронеж. 2020. С. 337–342.

2. Бречко А.А., Вершенник Е.В., и др. Взгляды командований зарубежных государств на проведение операции в киберпространстве // В сборнике: Проблемы технического обеспечения войск в современных условиях. Труды IV межвузовской научно-практической конференции. 2019. С. 132–136.

3. Коцыняк М.А., Лаута О.С., Иванов Д.А., Лукина О.М. Модель воздействия таргетированной кибернетической атаки на информационно-телекоммуникационную сеть // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 3–4 (129–130). С. 58–65.

4. Коцыняк М.А., Лаута О.С., Нечепуренко А.П. Модель системы воздействия на ин-

формационно-телекоммуникационную систему специального назначения в условиях информационного противоборства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 3–4 (129–130). С. 40–44.

5. Бухарин В.В., Семенов С.С., др. Техносферная война // Информационные системы и технологии. 2011. № 1 (63). С. 80–85.

6. Закалкин П.В., Иванов С.А. Взгляд вооруженных сил США на киберпространство // Состояние и перспективы развития современной науки по направлению «Информационная безопасность». Сборник статей II Всероссийской научно-технической конференции. Федеральное государственное автономное учреждение «Военный инновационный технополис «ЭРА». — Анапа. 2020. С. 18–22.

7. Бречко А.А., Вершенник Е.В. Проблемы использования киберпространства при проведении операций // В сборнике: Проблемы технического обеспечения войск в современных условиях. Труды IV межвузовской научно-практической конференции. 2019. С. 137–140.

8. Патент 2439691 Российская Федерация, МПК G06F 21/22 (2006.01). Способ защиты данных // Винокур Алекс (IL).; Заявитель и патентообладатель АКССАНА (ИЗРАЭЛЬ) ЛТД. (IL). 2009126283/08; заявл. 10.07.2009; опубл. 10.01.2012. бюл. № 1. 27 с.

9. Патент 2445686 Российская Федерация, МПК G06F 15/177 (2006.01) Способ установки, настройки, администрирования и резервного копирования программного обеспечения // Стручков И.В.; Заявитель и патентообладатель Стручков И.В. 2010102826/08; заявл. 21.01.2010; опубл. 27.07.2011. бюл. № 8. 24 с.

10. Патент 2445686 Российская Федерация, МПК G06F 15/177 (2006.01). Способ резервного копирования // Анисимов В.В., Бегаев А.Н., Стародубцев Ю.И., Вершенник Е.В., Чукариков А.Г.; Заявитель и патентообладатель Бегаев А.Н. 2017113265; заявл. 17.04.2017; опубл. 02.03.2018. бюл. № 7. 25 с.

11. Патент 2726318 Российская Федерация, МПК G06F 11/14 (2006.01), МПК G06F 12/00 (2006.01), МПК G06F 9/00 (2006.01). Способ резервного копирования состояния сложного объекта // Стародубцев Ю.И., Иванов С.А., Вершенник Е.В., Стародубцев П.Ю., Закалкин П.В., Шевчук А.Л.; Заявитель и патентообладатель Стародубцев Ю.И. 2020100724; заявл. 14.01.2020; опубл. 13.07.2020. бюл. № 20. 18 с.

12. ГОСТ Р 53111-2008 Устойчивость функционирования сети связи общего пользования. Требования и методы проверки.— М.: Стандартинформ. 2019. 15 с.

13. Патент 2623791 Российская Федерация, МПК G05B 23/00 (2006.01), МПК G06Q 10/04 (2012.01), Способ определения оптимальной периодичности контроля состояния процессов // Синев С.Г., Сорокин М.А., Стародубцев П.Ю., Сухорукова Е.В.; Заявитель и патентообладатель Стародубцев П.Ю. 2016102219; заявл. 25.01.2016; опубл. 29.06.2017. бюл. № 19. 13 с.

14. Starodubcev U.I., Vershennik E.V., Balenko E.G. Method of monitoring the state of communication networks // В сборнике: 2019 International Science and Technology Conference «EastConf», EastConf 2019. 2019. С. 8725400.

References

1. Starodubtsev Yu.I., Zakalkin P.V., Ivanov S.A. Problems of functioning of complex systems using cyberspace resources // In the collection: Radar, navigation, communication. Proceedings of the XXVI International Scientific and Technical Conference, in 6 vols. — Voronezh. 2020. P. 337–342.

2. Brechko A.A., Varsenik E.V., et al. Commands Views of foreign countries to conduct operations in cyberspace // In the collection: problems in the technical support of troops in modern conditions. Proceedings of the IV Interuniversity Scientific and Practical Conference. 2019. P. 132–136.

3. Kotsynyak M.A., Lauta O.S., Ivanov D.A., Lukina O.M. Model of the impact of a targeted cybernetic attack on the information and telecommunications network. Military Enginery. Issue 16. Counter-terrorism technical devices. 2019. № 3–4 (129–130). P. 58–65.

4. Kotsynyak M.A., Lauta O.S., Nechepurenko A.P. Model of the system of influence on the information and telecommunications system of special purpose in the conditions of information warfare // Military Enginery. Issue 16. Counter-terrorism technical devices. 2019. № 3–4 (129–130). P. 40–44.

5. Bukharin V.V., Semenov S.S., et al. Technosphere war // Information Systems and Technologies. 2011. № 1 (63). P. 80–85.

6. Zakalkin P.V., Ivanov S.A. Opinion of the armed forces of the United States in cyberspace // The state and prospects of development of modern science in the field of «Information Security». Collection of articles of the II All-Russian Scientific and Technical Conference. Federal State Autonomous Institution «Military Innovation Technopolis «ERA». — Anapa. 2020. P. 18–22.

7. Brechko A.A., Vershennik E.V., et al. Problems of using cyberspace during operations // In the collection: Problems of technical support of troops in modern conditions. Proceedings of the IV Interuniversity Scientific and Practical Conference. 2019. P. 137–140.

8. Patent 2439691 Russian Federation, IPC G06F 21/22 (2006.01). Method of data protection // Vinokur Alex (IL).; Applicant and patent holder AKSSANA (ISRAEL) LTD. (IL). 2009126283/08; declared on 10.07.2009; published on 10.01.2012. byul. № 1. 27 p.

9. Patent 2445686 Russian Federation, IPC G06F 15/177 (2006.01). Method of installation, configuration, administration and backup of software // Struchkov I.V.; Applicant and patent holder Struchkov I.V. 2010102826/08; application 21.01.2010; publ. 27.07.2011. byul. № 8. 24 p.

10. Patent 2445686 Russian Federation, IPC G06F 15/177 (2006.01). Backup method // Anisimov V.V., Begaev A.N., Starodubtsev Yu.I., Vershennik E.V., Chukarikov A.G.; Applicant and patent holder Begaev A.N. 2017113265; application form 17.04.2017; publ. 02.03.2018. byul. № 7. 25 p.

11. Patent 2726318 Russian Federation, IPC G06F 11/14 (2006.01), IPC G06F 12/00 (2006.01), IPC G06F 9/00 (2006.01). Method for backing up the state of a complex object // Starodubtsev Yu.I., Ivanov S.A., Vershennik E.V., Starodubtsev P.Yu., Zakalkin P.V., Shevchuk A.L.; Applicant and patent holder Starodubtsev Yu.I. 2020100724; application 14.01.2020; publ. 13.07.2020. byul. № 20. 18 p.

12. GOST R 53111-2008 Stability of the functioning of the public communication network. Requirements and verification methods. — M.: Standartinform. 2019. 15 p.

13. Patent 2623791 Russian Federation, IPC G05B 23/00 (2006.01), MPK G06Q 10/04 (2012.01), a Method of determining the optimal frequency control of processes // Sinev S.G., Sorokin M.A., Starodubtsev P.J., Sukhorukov E.V.; Applicant and patentee Starodubtsev P.Y. 2016102219; Appl. 25.01.2016; publ. 29.06.2017. bull. № 19. 13 p.

14. Starodubcev U.I., Vershennik E.V., Balenko E.G. Method of monitoring the state of communication networks // In the collection: 2019 International Science and Technology Conference «EastConf», EastConf 2019. 2019. S. 8725400.