РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ РАЗВЕРТЫВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ ЦЕНТРА УПРАВЛЕНИЯ ПОЛЕТАМИ КОСМИЧЕСКИХ АППАРАТОВ

М. А. Прохоров¹, А. Ю. Цветков¹, А. А. Толмачев² ✉

¹ Военно-космическая академия им. А. Ф. Можайского,
г. Санкт-Петербург, Российская Федерация

² Военная академия воздушно-космической обороны им. Маршала Советского Союза Г. К. Жукова,
г. Тверь, Российская Федерация

В настоящее время повседневная и боевая деятельность практически любой армии мира во многом определяется качеством информационно-космического обеспечения. При этом качество обеспечения во многом зависит от устойчивости функционирования таких уникальных технических объектов, как центры управления полетами космических аппаратов. Исходя из особенностей построения новых и модернизации уже существующих центров управления полетами установлена их восприимчивость к деструктивным информационным воздействиям. В связи с этим был определен единственный способ гарантированного восстановления информационно-управляющей системы после информационно-технического воздействия, а именно полное переразвертывание автоматизированных рабочих мест, включающее переустановку операционных систем, общего программного обеспечения и специального программного обеспечения. Для обеспечения оперативности восстановления рассматриваемой системы была обоснована необходимость автоматизации процесса развертывания программного обеспечения автоматизированных рабочих мест центра управления полетами космических аппаратов. Результаты проведенного анализа существующих подходов к развертыванию программного обеспечения показали необходимость реализации непосредственно дистрибутивных методов. Исходя из этого был произведен объектно-ориентированный анализ процесса развертывания программного обеспечения, а также предложена структура автоматизированной системы развертывания программного обеспечения автоматизированных рабочих мест центра управления полетами космических аппаратов, применение которой позволит обеспечить необходимый уровень устойчивости выполнения технологических циклов управления космическими аппаратами в частности, и качество информационно-космического обеспечения войск в целом.

Ключевые слова: автоматизированная система, деструктивное информационное воздействие, развертывание программного обеспечения, оперативность, устойчивость инфраструктуры.

Введение

Результаты анализа военных конфликтов последних десятилетий показывают непреклонное возрастание роли информационно-космического обеспечения в вооруженных силах любого технологически развитого государства мира. При этом, под информационно-космическим обеспече-

нием (ИКО) понимается совокупность действий (мероприятий), выполняемых как самостоятельно, так и во взаимодействии с потребителями космических войск (органами управления различного уровня, силами ракетно-космической обороны в части, касающейся контроля космического пространства, и системы предупреждения о ракетном нападении, силами запуска космических аппаратов (КА), силами управления КА), а также космическими силами и средствами видов Вооруженных сил Российской Федерации (ВС РФ) по [1]:

✉ the_lexys@bk.ru

© Ассоциация «ТП «НИСС», 2020

- поддержанию устойчивого функционирования каналов космической связи;
- формированию навигационного поля;
- созданию на борту КА изображений (в виде скрытого изображения на фотопленке, записи радиоголограммы, записи оптико-электронного изображения с матрицы и др.);
- доведению до приемных пунктов наземных специальных комплексов специальных материалов и сигналов с требуемым качеством;
- контролю фоно-целевой обстановки и космической деятельности иностранных государств в стратегической космической зоне;
- контролю пусков ракет;
- измерению, записи и передаче значений параметров космического пространства (радиационной обстановки, магнитного поля и др.) в интересах информационного обеспечения применения ВС РФ.

Для качественного решения задач ИКО созданы космические комплексы (КК) и космические системы (КС) различного целевого назначения [2]. В настоящее время эффективное функционирование указанных систем в различных условиях обстановки продолжает определяться, в значительной степени, состоянием и работоспособностью таких уникальных объектов, как центры управления полетами космических аппаратов (ЦУП КА) [3], в которых в автоматизированном режиме накапливается информация о состоянии орбитальной группировки КА и вырабатываются управляющие воздействия на КА в соответствии с их целевым предназначением и программой полета. Современные ЦУП КА справедливо воспринимать как «технологическое сердце» любой КС. Данное обстоятельство предопределяет их в качестве приоритетных целей для потенциального противника [4].

Следует отметить, что современные ЦУП КА строятся по принципу открытых систем [5], что обуславливает их восприимчивость к информационно-техническим воздействиям (ИТВ), в частности к деструктивным программным воздействиям. Технологии проведения ИТВ подробно рассмотрены в работах [6–9].

В настоящее время большинство специалистов в области информационной безопасности автоматизированных систем специального назначения сходятся во мнении, что единственным гарантированным способом восстановления информационно-управляющей системы после ИТВ является полное переразвертывание автоматизированных рабочих мест, включающее переустановку операционных систем (ОС), общего программного обеспечения (ОПО) и специального программного обеспечения (СПО).

В связи с этим, задача обеспечения оперативности восстановления ЦУП КА после ИТВ становится все актуальнее.

1. Постановка задачи автоматизации развертывания программного обеспечения автоматизированных рабочих мест центра управления полетами космических аппаратов

Современные ЦУП КА организуются на базе ряда специализированных программно-технических комплексов (ПТК) [10]:

- ПТК баллистического обеспечения (прием и обработка текущих навигационных параметров, расчет баллистических характеристик КА, подготовка массивов командно-программной информации, расчет начальных условий и выдача их потребителям, расчет зон радиовидимости);

- ПТК планирования (подготовка средств наземного комплекса управления в соответствии с технологическим циклом управления, корректировка плана в зависимости от состояния отдельных КА, формирование технологических данных для проведения сеансов связи, расчет программ управления и массивов командно-программной информации);

- ПТК телеметрического обеспечения (прием и обработка телеметрической информации (ТМИ), прием и обработка отчетов бортовых цифровых вычислительных машин, выполнение автоматизированного обобщенного контроля, отображение результатов обработки ТМИ, передача ТМИ удаленным центрам анализа);

- ПТК управления (проведение текущего сеанса управления КА, закладка командно-программной, служебной информации, контроль выполнения программы управления по поступающей ТМИ и квитанциям, оперативное руководство станциями приема контрольно-измерительных систем).

Структурными элементами функциональных секторов являются автоматизированные рабочие места (АРМ), функционирующие под управлением Unix-подобных ОС (MCBC, Astra Linux и др.), ОПО и СПО, при этом количество АРМ варьируется от десятка до нескольких десятков, в зависимости от особенностей реализуемых технологических циклов управления КА и состава орбитальной группировки. Исходя из размерности и специфики используемого программного обеспечения (ПО) зачастую становится невозможным выполнить требования по оперативности восстановления ЦУП КА после ИТВ путем развертывания эталонных конфигураций АРМ, предъявляемых эксплуатационной документацией и другими регламентирующими документами.

В настоящее время существует несколько способов развертывания АРМ, отличающихся разным уровнем автоматизации и унификации [11]:

1. Клонирование итоговой установки одного АРМ на несколько дисков. Несомненным плюсом

подхода является его универсальность, минусом подхода являются, во-первых, необходимость совпадения конфигурации аппаратной части АРМ, во-вторых, на всех АРМ абсолютно точно копируются все пароли, в том числе SSH-ключи (ключи идентификации для сетевого протокола прикладного уровня), что обуславливает в случае компрометации одного АРМ компрометацию всей системы в целом.

2. Клонирование по сети. Основным преимуществом подхода является оперативность развертывания, однако сохраняются недостатки предыдущего подхода.

3. Дистроспецифичные подходы, позволяющие использовать технологию загрузки компьютера с помощью сетевой карты без использования локальных носителей данных Preboot eXecution Environment (PXE) и обеспечивающие возможность гибкой конфигурации АРМ. Основной недостаток подхода заключается в многоуровневости и определенной сложности реализуемого процесса.

Исходя из результатов анализа существующих подходов к развертыванию АРМ становится очевидна необходимость разработки автоматизированной системы развертывания (АСР) ПО, реализующей дистроспецифичный подход. Для этого с целью выявления подлежащих автоматизации аспектов на начальном этапе необходимо разработать модель процесса развертывания ПО АРМ ЦУП КА.

2. Разработка модели процесса развертывания программного обеспечения автоматизированных рабочих мест центра управления полетами космических аппаратов

Рациональная разработка АСР ПО возможна лишь на основе результатов глубокой предварительной аналитической проработки.

В настоящее время разработано множество методологий моделирования процессов [12]. С целью описания сложноформализуемого процесса развертывания ПО на АРМ ЦУП КА, выявления подлежащих автоматизации аспектов и строгого сопоставления каждого автоматизируемого аспекта (шага) соответствующей функцией разрабатываемой системы, наиболее полно подходит унифицированный язык графического объектного описания UML (Unified Modeling Language).

Непосредственно перед разработкой интересующей нас модели необходимо ввести следующее допущение: процесс развертывания ПО АРМ ЦУП КА рассматривается с точки зрения его повторяемости во времени и потребности в автоматизации. На начальном этапе моделирования, в соответствии с нотацией UML, необходимо разработать диаграмму видов деятельности (activity diagrams) в рамках рассматриваемого прецедента (рис. 1).

Рис. 1. Общий вид процесса развертывания ПО АРМ ЦУП КА (activity diagrams)

На представленной структуре также выделены процессы, подлежащие автоматизации с целью обеспечения оперативности развертывания ПО АРМ ЦУП КА:

- подготовка АРМ к развертыванию ПО и СПО (P2);
- развертывание ОС на АРМ с учетом ролей (P3);
- первоначальная настройка ОС в соответствии с требованиями (P4);

- развертывание СПО на АРМ с учетом ролей (P5).

Для задания конкретных требований к разрабатываемой системе необходимо осуществить сопоставление каждому автоматизируемому шагу соответствующих функций системы с последующей конкретизацией частного требования.

Это отражается в рамках функциональной модели, реализуемой посредством диаграммы use-case (рис. 2).

Рис. 2. Функциональная модель АСП ПО АРМ ЦУП КА (use-case)

Для удовлетворения синтезированных требований к разрабатываемой АСП ПО АРМ ЦУП КА (с учетом использования Unix-подобных ОС) необходимо основываться на использовании технологии PXE и применении файлов ответов – pressed-файлов с расширенным функционалом.

3. Разработка структуры автоматизированной системы развертывания программного обеспечения автоматизированных рабочих мест центра управления полетами космических аппаратов

В настоящее время наиболее используемой при создании и модернизации ЦУП КА стала отечественная ОС семейства Unix – Astra Linux (отметим, что на сегодняшний день это единственная система с запатентованными средствами защиты информации [13]). Исходя из этого, была разработана структура АСП ПО АРМ ЦУП КА, состоящая из следующих модулей:

- модуль формирования эталонных файлов-ответов. Должен обеспечивать получение, хранение и изменение соответствующих сущностей (pressed*.cfg) для каждого АРМ инфраструктуры (взаимодействие через SSH). Кроме того, должна быть реализована возможность редактирова-

ния параметра pressed/late_command для каждого полученного файла-ответа с целью организации импорта дополнительных настроек ОС по окончании установки;

- модуль управления форматированием носителей информации на удаленных АРМ. Должен обеспечивать возможность запуска соответствующих скриптов посредством сетевого протокола SSH, при этом не должно осуществляться копирования самого скрипта на АРМ;

- модуль управления раздачей репозитория ОС. Должен обеспечивать привязку mac-адресов АРМ к соответствующим pressed-файлам, хранящимся в ранее созданной базе данных. Для этого необходимо, чтобы все сетевые карты АРМ инфраструктуры поддерживали технологию PXE, а также, чтобы были установлены и настроены пакеты isc-dhcp-server и vsftpd (входят в дистрибутив Astra Linux SE) на сервере установки;

- модули управления раздачей репозитория СПО и скриптов дополнительной настройки ОС. Их целесообразно создавать на базе высоконадежного сервера Apache (входит в дистрибутив Astra Linux SE). Существует несколько способов организации репозитория СПО, однако для полноценного хранилища deb-пакетов в локальной сети рекомендуется использовать APT-MIRROR (также входящего в дистрибутив Astra Linux SE). Модуль управления скриптами дополнительной настройки

ОС должен позволять создавать, редактировать и хранить скрипты (postinstall*.sh) для каждого АРМ инфраструктуры.

Опираясь на разработанную структуру, АСР ПО была реализована в виде самостоятельного аппаратно-программного компонента (АПК). АПК был выполнен на базе дополнительного АРМ

(форм-фактор ноутбук), временно подключаемого к инфраструктуре ЦУП КА.

Предлагаемый вариант интеграции перспективной АСР ПО АРМ не потребует существенных дополнительных экономических издержек, как для вновь разрабатываемых, так и для существующих (модернизируемых) ЦУП КА (рис. 3).

Рис. 3. Структура АПК, реализующего функции АР ПО

Следует отметить, что реализованный АПК также позволяет контролировать целостность и авторство разворачиваемого ПО за счет передачи подписанных дистрибутивов и последующей проверки электронных подписей. Кроме того, лежащий в основе компонента дистрибутивный подход позволяет учитывать интегрированные связи в инфраструктуре ЦУП КА, что обеспечивает целостность полной конфигурации ПО.

4. Оценка эффективности разработанной системы развертывания программного обеспечения автоматизированных рабочих мест центра управления полетами космических аппаратов

Для определения степени выполнения требований по оперативности развертывания эталонных конфигураций АРМ был применен метод построения и расчета сетевых графиков работ, выполняемых соответствующим персоналом объекта информатизации.

При исследовании эффективности разработанной системы рассматривался типовый объект информатизации (состоящий из трех АРМ), на котором проводилось развертывание ОС Astra Linux «Орел» и дополнительного программного обеспечения VirtualBox силами одного специалиста. В качестве допущений было принято полное функциональное подобие АРМ. Располагаемое время завершения работ составило 90 минут.

Исходя из того, что процессы по развертыванию состоят из множества мероприятий, то согласно центральной предельной теореме теории вероятностей можно с достаточным основанием считать, что распределение времени завершения всего комплекса работ подчиняется нормальному закону. Это, в свою очередь, позволило использовать график, представляющий собой значения интегральной функции нормального распределения. Входом в график служила величина нормировочной переменной X . На выходе из графика считывалось значение P – вероятность завершения всего комплекса работ за заданное время.

В результате исследования были получены следующие показатели эффективности разработанной системы, представленные в табл.

Таблица

Результаты исследования оперативности развертывания ПО АРМ

Выполняемые работы	X – нормировочная переменная		P – вероятность своевременного развертывания	
	Ручной способ	АПК	Ручной способ	АПК
Развертывание эталонных конфигураций АРМ	–29,3	1,6	≈ 0	0,97

Полученные результаты наглядно показывают предпочтительность применения разработанного АПК по критерию оперативности.

Заключение

Разработанная АСР ПО АРМ, в отличие от известных [14], строится на основе входящих в дистрибутив пакетов ОС специального назначения и позволяет развертывать полнофункциональные АРМ (включая СПО и дополнительные настройки) за требуемое время, что, в свою очередь,

позволяет обеспечить устойчивость выполнения технологических циклов управления КА в любых условиях обстановки.

Следует также отметить, что применение предложенного АПК с целью недопущения деструктивных ИТВ целесообразно непосредственно после выполнения соответствующих комплексов организационно-технических мероприятий, направленных на противодействие несанкционированному доступу, и определенными, в свою очередь, руководящими документами и эксплуатационной документацией объектов информатизации.

Список литературы

- [1] Остапенко О. Н., Баушев С. В., Морозов И. В. Информационно-космическое обеспечение группировок войск (сил) ВС РФ : учеб.-науч. издание. СПб. : Любавич, 2012. 368 с.
- [2] Мануйлов Ю. С., Калинин В. Н., Гончаревский В. С., Делий И. И., Новиков Е. А. Управление космическими аппаратами и средствами наземного комплекса управления. СПб. : ВКА имени А.Ф. Можайского, 2010. 609 с.
- [3] Чашин С. В., Вечеркин В. Б., Гончаров А. М. Алгоритм оценивания живучести комплексов систем автоматизации и его элементов в условиях деструктивных воздействий // Телекоммуникационные технологии. 2016. № 14. С. 122–125.
- [4] Прохоров М. А. Оценка устойчивости центра управления полетами космических аппаратов в условиях деструктивных воздействий // Труды науч.-практ. конф. «Проблемы технического обеспечения войск в современных условиях». Военная академия связи. 2017. С. 160–164.
- [5] Криков А. П., Квасов М. Н., Прохоров М. А. Практические рекомендации по обеспечению устойчивости функционирования автоматизированных систем специального назначения критически важными объектами в условиях деструктивных информационных воздействий // Известия Тульского государственного университета. Технические науки. Вып. 6. 2019. С. 14–21.
- [6] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]. URL: www.bdu.fstec.ru/documents/16 (дата обращения: 10.01.2020).
- [7] Пискунов И. В. Цепочка Cyber-kill Chain: от моделирования до проектирования защищенного периметра [Электронный ресурс]. URL: https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/325123.php (дата обращения: 12.01.2020).
- [8] Макаренко С. И. Проблемы и перспективы применения кибернетического оружия в современной сетевой войне // Спецтехника и связь. 2011. № 3. С. 41–47.
- [9] Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетевых войнах начала XXI века. Монография. СПб. : Научно-технологические исследования, 2017. 546 с.
- [10] Некрасов М. В., Пакман Д. Н., Антамошкин А. Н. Методы унификации современных средств обработки телеметрической информации в центрах управления полетами космических аппаратов // Вестник СибГАУ. 2014. № 1 (53). С. 48–53.
- [11] Развертывание различных дистрибутивов Linux в корпоративной среде [Электронный ресурс]. URL: <https://haker.ru/2014/10/06/linux-in-corp/> (дата обращения: 13.01.2020).
- [12] Чернышов А. С. Анализ методов моделирования автоматизированных систем // Материалы X Всеросс. науч.-практ. конф. студентов, аспирантов, работников образования и промышленности. 2019. С. 367–370.
- [13] Буренин П. В., Девянин П. Н., Лебеденко Е. В., Проскуриков В. Г., Цибуля А. Н. Безопасность операционной системы специального назначения Astra Linux Special Edition : учеб. пособ. для вузов. М. : Горячая линия – Телеком, 2016. 312 с.
- [14] Кузьмицкий А. Автоматическая установка «Astra Linux Special Edition» (часть 2) [Электронный ресурс]. URL: http://lab50.net/auto_install_astra_linux_part2/ (дата обращения: 13.01.2020).

DEVELOPMENT OF AN AUTOMATED SYSTEM FOR DEPLOYING SOFTWARE FOR AUTOMATED WORKSTATIONS OF THE SPACECRAFT FLIGHT CONTROL CENTER

M. A. Prokhorov¹, A. Yu. Tsvetkov¹, A. A. Tolmachev²

¹ *Mozhaisky Military Space Academy, Saint Petersburg, Russian Federation*

² *Military Aerospace Defense Academy, Tver, Russian Federation*

At present, the daily and combat activities of almost any army in the world are largely determined by the quality of information and space support. At the same time, the quality of support depends largely on the stability of the functioning of such unique technical facilities as spacecraft flight control centers. Based on the features of building new and upgrading existing flight control centers, their susceptibility to destructive information influences has been established. In this regard, the only way to guarantee the recovery of the information management system after information and technical impact was determined, namely, the complete re-deployment of automated workplaces, including the reinstalling of operating systems, general software and special software. To ensure the efficiency of recovery of the system under consideration, the need to automate the deployment of software for automated workstations of the spacecraft flight control center was justified. The results of the analysis of existing approaches to software deployment have shown the need for implementation directly disrespecting methods. Based on this, the complex software deployment process was formalized, and the structure of the automated software deployment system for automated workstations of the spacecraft flight control center was proposed, the use of which will ensure the necessary level of stability in the implementation of technological cycles of spacecraft control in particular, and the quality of information and space support for troops in General.

Keywords: automated system, destructive information impact, software deployment, efficiency, infrastructure stability.

References

- [1] Ostapenko O. N., Baushev S. V., Morozov I. V. *Informacionno-kosmicheskoe obespechenie gruppirovok vojsk (sil) V/S RF* [Information and space support for troops (forces) of the RF Armed Forces]. Saint-Petersburg, Lyubavich, 2012, 368 p. (In Russian)
- [2] Manuilov Yu. S., Kalinin V. N., Goncharevsky V. S., Deliy I. I., Novikov E. A. *Upravlenie kosmicheskimi apparatami i sredstvami nazemnogo kompleksa upravleniya* [Spacecraft and ground control complex control]. Saint-Petersburg, WKA named after A. F. Mozhaysky, 2010, 609 p. (In Russian)
- [3] Chashchin S. V., Vecherkin V. B., Goncharov A. M. *Algoritm ocenivaniya zhivuchesti kompleksov sistem avtomatizatsii i ego elementov v usloviyah destruktivnykh vozdeystviy* [Algorithm for assessing the survivability of complexes of automation systems and its elements under conditions of destructive influences] // *Telecommunication technologies*, 2016, no. 14, pp. 122–125. (In Russian)
- [4] Prokhorov M. A. *Ocenivanie ustojchivosti centra upravleniya poletom kosmicheskikh apparatov v usloviyah destruktivnykh vozdeystviy* [Estimation of stability of the spacecraft flight control center under the conditions of destructive influences] // *Transactions of scientific and practical conference «Problems of technical support of troops in modern conditions»*, Military Academy of Communications, 2017, pp. 160–164. (In Russian)
- [5] Krikov A. P., Kvasov M. N., Prokhorov M. A. *Prakticheskie rekomendatsii po obespecheniyu ustojchivosti funkcionirovaniya avtomatizirovannykh sistem special'nogo naznacheniya kriticheski vazhnymi ob'ektami v usloviyah destruktivnykh informacionnykh vozdeystviy* [Practical recommendations for ensuring the stability of the functioning of automated systems for special purposes with critical objects under the conditions of destructive information impacts] // *Bulletin of Tula State University. Technical Science*, vol. 6, 2019, pp. 14–21. (In Russian)
- [6] *Bazovaya model' ugroz bezopasnosti personal'nykh dannykh pri ih obrabotke v informacionnykh sistemakh personal'nykh dannykh* [Basic model of personal data security threats when they are processed in personal data information systems]. Available at: www.bdu.fstec.ru/documents/16 (accessed 01.10.2020). (In Russian)

- [7] Piskunov I. V. *Cepochka Cyber-kill Chain: ot modelirovaniya do proektirovaniya zashchishchennogo perimetra* [Cyber-kill Chain: from modeling before designing a secure perimeter]. Available at: https://www.securitylab.ru/blog/personal/Informacionnaya_bezопасnost_v_detalyah/325123.php (accessed 12.01.2020). (In Russian)
- [8] Makarenko S. I. *Problemy i perspektivy primeneniya kiberneticheskogo oruzhiya v sovremennoj setecentricheskoj vojne* [Problems and prospects of the use of cybernetic weapons in modern network-centric warfare] // *Special equipment and communications*, 2011, no. 3, pp. 41–47. (In Russian)
- [9] Makarenko S. I. *Informacionnoe protivoborstvo i radioelektronnaya bor'ba v setecentricheskih voynah nachala XXI veka* [Information confrontation and electronic warfare in network-centric wars of the beginning of the XXI century]. Saint Petersburg, High Technologies, 2017, 546 p. (In Russian)
- [10] Nekrasov M. V., Pakman D. N., Antamoshkin A. N. *Metody unifikacii sovremennyh sredstv obrabotki teletricheskoj informacii v centrakh upravleniya poletami kosmicheskikh apparatov* [Methods for the unification of modern means of processing telemetric information in spacecraft flight control centers] // *Vestnik SibGAU*, 2014, no. 1 (53), pp. 48–53. (In Russian)
- [11] *Razvertyvanie razlichnyh distributivov Linux v korporativnoj srede* [Deploying various Linux distributions in a corporate environment]. Available at: <https://xakep.ru/2014/10/06/linux-in-corp/> (accessed 13.01.2020). (In Russian)
- [12] Chernyshov A. S. *Analiz metodov modelirovaniya avtomatizirovannykh sistem* [Analysis of modeling methods for automated systems] // *Materials X All-Russian scientific and practical conference of students, graduate students, educators and industry*, 2019, pp. 367–370. (In Russian)
- [13] Burenin P. V., Devyanin P. N., Lebedenko E. V., Proskurikov V. G., Tsibulya A. N. *Bezопасnost' operacionnoj sistemy special'nogo naznacheniya Astra Linux Special Edition* [Security of the special-purpose operating system Astra Linux Special Edition]. Moscow, Goryachaya liniya – Telecom, 2016, 312 p. (In Russian)
- [14] Kuzmitsky A. *Avtomaticheskaya ustanovka «Astra Linux Special Edition» (chast' 2)* [Automatic installation of «Astra Linux Special Edition» (part 2)]. Available at: http://lab50.net/auto_install_astra_linux_part2/ (accessed 13.01.2020). (In Russian)

Сведения об авторах

Прохоров Михаил Александрович – кандидат технических наук, начальник лаборатории военного института (научно-исследовательского) Военно-космической академии им. А. Ф. Можайского. Окончил Военно-космическую академию им. А. Ф. Можайского в 2010 году. Область научных интересов: системный анализ, автоматизированные системы управления, устойчивость информационных систем.

Толмачев Алексей Александрович – кандидат военных наук, старший преподаватель кафедры основ построения радиоэлектронных средств и систем Военной академии воздушно-космической обороны им. Маршала Советского Союза Г. К. Жукова. Окончил Военно-космическую академию им. А. Ф. Можайского в 2008 году. Область научных интересов: теория эффективности, исследование операций, системный анализ, автоматизированные системы управления.

Цветков Александр Юрьевич – кандидат технических наук, доцент кафедры Военно-космической академии им. А. Ф. Можайского. Окончил Ростовский военный институт ракетных войск им. Главного маршала артиллерии М. И. Неделина в 2000 году. Область научных интересов: автоматизированные системы управления.