СТАНДАРТИЗАЦИЯ ВОЕННОЙ ТЕХНИКИ

2/2024

Кибербезопасность. Основные тенденции

Требования к специальным техническим средствам противодействия беспилотным устройствам

Применение терминологических стандартов в жизненном цикле изделий перспективной авиационной техники

«ВАЖНО ПРОДОЛЖАТЬ НАРАЩИВАТЬ РИТМИЧНОЕ ОБЕСПЕЧЕНИЕ ВООРУЖЕННЫХ СИЛ СОВРЕМЕННЫМ, ВЫСОКОТЕХНОЛОГИЧНЫМ ОРУЖИЕМ И ТЕХНИКОЙ. ЭТО БЕСПИЛОТНЫЕ АВИАЦИОННЫЕ И НАЗЕМНЫЕ КОМПЛЕКСЫ, ВЫСОКОТОЧНЫЕ СРЕДСТВА ПОРАЖЕНИЯ, СРЕДСТВА РЭБ И СИСТЕМЫ КОНТРБАТАРЕЙНОЙ БОРЬБЫ, ЭТО РАЗЛИЧНЫЕ ВИДЫ СВЯЗИ ДЛЯ УСТОЙЧИВОГО И НЕПРЕРЫВНОГО УПРАВЛЕНИЯ И ДРУГАЯ НОМЕНКЛАТУРА <...>

С 2021 ГОДА ПО 2023-Й <...> РОСТ СОСТАВИЛ ПО РАКЕТНО-АРТИЛЛЕРИЙСКОМУ ВООРУЖЕНИЮ БОЛЕЕ ЧЕМ В 22 РАЗА, ПО СРЕДСТВАМ РАДИОЭЛЕКТРОННОЙ БОРЬБЫ И РАЗВЕДКИ – В 15 РАЗ, ПО БОЕПРИПАСАМ И СРЕДСТВАМ ПОРАЖЕНИЯ – В 14 РАЗ, ПО АВТОМОБИЛЯМ – В СЕМЬ РАЗ, ПО СРЕДСТВАМ ИНДИВИДУАЛЬНОЙ БРОНЕЗАЩИТЫ – В ШЕСТЬ РАЗ, ПО АВИАЦИОННОЙ ТЕХНИКЕ И БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТАМ – В ЧЕТЫРЕ РАЗА, ПО БРОНЕТАНКОВОМУ ВООРУЖЕНИЮ – ПОЧТИ В 3,5 РАЗА».

В.В. Путин, Президент Российской Федерации,
из вступительного слова на встрече
с руководителями предприятий ОПК
(Московская область, Королев, 25 мая 2024 года)

Источник http://kremlin.ru

Уважаемые коллеги!

Сквозной темой очередного номера журнала «Стандартизация военной техники» стала авиационная техника и беспилотные устройства в частности. Сегмент беспилотных воздушных судов находится на подъеме, спрос на такие изделия растет во всем мире, что не случайно. Беспилотники значительно облегчают решение технических задач. Широкое применение устройства находят не только в военной, но и в других областях, где их использование становится все более востребованным, а зачастую и необходимым.

Конкурентные преимущества в данной сфере во многом определяются значением, которое придается стандартизации в жизненном цикле изделий авиационной промышленности. От терминологических стандартов, применяемых на всех этапах производства и эксплуатации устройств, зависят и безопасность полетов, и качество выпускаемой продукции. К обязательным условиям управления качеством, своевременной разработки перспективной техники эксперты относят также унификацию на производстве.

Не менее важная роль отводится требованиям, предъявляемым к современным беспилотным воздушным судам и специальным техническим средствам противодействия им, а также регламентам проверки функциональности устройств на конкретных объектах с гарантированным результатам. В статьях, опубликованных на страницах этого номера, эксперты заостряют внимание на задачах, требующих первоочередного решения, вариантах и методиках их решения. Большое внимание уделяется лучшим практикам и опыту зарубежных стран в области стандартизации продукции военно-промышленного комплекса.

Поступательное развитие высокотехнологичных сегментов в условиях цифровизации невозможно без обеспечения кибербезопасности, которая до недавнего времени считалась отдельным направлением информационной безопасности. Однако уровень задач, требующих комплексного решения, позволяет специалистам заявить о том, что эта междисциплинарная наука занимает промежуточное положение между информационными технологиями и другими дисциплинами, связанными с бизнесом, предпринимательством, правом и т. д. Анализ ключевых тенденций в этой сфере способствует разработке концепции кибербезопасности, предусматривающей использование современных технологий, например, искусственного интеллекта, и инструментов, реализованных на базе отечественных программно-аппаратных комплексов.

По традиции желаем вам интересного и познавательного чтения.

РЕДАКЦИЯ ЖУРНАЛА

РОССИЙСКИЙ ИНСТИТУТ СТАНДАРТИЗАЦИИ

ЖУРНАЛ

СТАНДАРТИЗАЦИЯ ВОЕННОЙ ТЕХНИКИ 2/2024

ИЗДАТЕЛЬ

Федеральное государственное бюджетное учреждение «Российский институт стандартизации»

Российская Федерация,
117418 г. Москва, Нахимовский пр-т, д. 31, корп. 2

Журнал является периодическим текстовым электронным изданием.

Форма распространения – сетевое издание.

РЕДАКЦИЯ

Руководитель К.В. Костылева
Литературный редактор С.П. Арянина
Верстка А.О. Баркару
Корректура Л.С. Лысенко

АДРЕС РЕДАКЦИИ

Российская Федерация,
117418, Москва,
Нахимовский пр-т, д. 31, корп. 2
+7 (495) 531-26-03

Выпуск журнала «Стандартизация военной техники» возобновлен в 2023 году во исполнение пункта 40 Плана мероприятий («дорожной карты») развития стандартизации в Российской Федерации на период до 2027 года, утвержденного Заместителем Председателя Правительства Российской Федерации Д.Н. Козаком от 15 ноября 2019 г. № ДК-П7-9914.

Издается Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации»).

Журнал осуществляет публикацию материалов по актуальным вопросам стандартизации военной техники с целью обмена опытом между специалистами, а также информационного и методического обеспечения работ по стандартизации оборонной продукции.

Мнение редакции может не совпадать с мнением авторов.

Перепечатка материалов допускается только с письменного согласия редакции.

При использовании материалов ссылка на журнал обязательна.

Подписано в печать 28.06.2024
Дата выхода в свет 28.06.2024
Формат 60 × 90 1/8.
Усл. печ. л. 4,63.

СОДЕРЖАНИЕ

ИНФОРМАЦИОННАЯ ЗАЩИТА

Кибербезопасность. Основные тенденции

***Алексей Бурый**, д-р техн. наук, эксперт РАН, Российский институт стандартизации* 4

Информационный анализ эффективности радиопротиводействия беспилотным воздушным судам

***Андрей Сухов**, д-р техн. наук, профессор, ведущий научный сотрудник ФКУ НПО «СТиС» МВД России, Российский институт стандартизации*

***Сергей Пузийчук**, начальник центра ФКУ НПО «СТиС МВД России* 14

БЕЗОПАСНОСТЬ

Требования к специальным техническим средствам противодействия беспилотным устройствам: алгоритм разработки и исполнения

***Олег Пелипас**, начальник отдела информационной безопасности Российского института стандартизации* 25

ОТРАСЛЕВЫЕ СТАНДАРТЫ

К вопросу применения терминологических стандартов в жизненном цикле изделий перспективной авиационной техники

***Никита Куприков**, канд. техн. наук, доцент, старший научный сотрудник Института 9 Московского авиационного института (НИУ), главный специалист сектора научно-экспертных работ Российского института стандартизации* 30

АЛЕКСЕЙ БУРЫЙ,
д-р техн. наук, эксперт РАН, Российский институт стандартизации

КИБЕРБЕЗОПАСНОСТЬ. ОСНОВНЫЕ ТЕНДЕНЦИИ

Успех современных военных операций во многом определяется технологиями, которые, в свою очередь, диктуют направления совершенствования вооружения и военной техники и, как следствие, стратегий ведения боевых действий. Автоматизированные системы управления технологическими процессами (АСУ ТП) критически важных объектов (КВО) находятся под угрозой как со стороны обычных вирусов, так и целенаправленных атак.

Работа носит концептуальный характер – подчеркивается важность кибербезопасности как стратегического направления поддержки информационно-коммуникационных технологий, одновременно отражая необходимость в постоянно совершенствуемых методах обеспечения безопасности в целях разработки единого методологического подхода к информационной защите нынешней и будущей инфраструктуры современного общества.

Начало XXI века ознаменовалось формированием новой цифровой реальности, которая наряду с очевидным улучшением качества жизни человечества существенно сузила пространство безопасности информационной инфраструктуры. Комплекс качественно новых угроз и вызовов поставил в международную повестку вопрос об объединении усилий многих стран в деле обеспечения надежной защиты цифровой среды, как внутренней, так и глобальной [3].

На уровне Организации Североатлантического договора (далее – НАТО) кибербезопасность стала институциональной политикой. Кибербезопасность отражает элементы безопасности в виртуальном мире Интернета. Кибербезопасность, на самом базовом уровне, заключается в обеспечении защиты от (а) кибератак – попыток нарушить работу, задержать или уничтожить компьютерные сети [13].

Если на первых порах целями киберпреступлений становились промышленные объекты, инновационные технологии [12], то теперь, помимо «естественного фона» интереса к вопросам оборонного комплекса [1, 2], критически важным объектам [5], злоумышленники все чаще рассматривают и социальные объекты как потенциальные мишени своего воздействия [9], например, биометрические технологии в процессах взаимодействия банк – клиент (в ходе идентификации и подтверждения финансовых операций клиентами) [11].

За сравнительно небольшое время кибербезопасность из отдельного направления информационной безопасности все больше заявляет о себе как о междисциплинарной науке, занимающей промежуточное положение между информационными технологиями (ИТ) и другими ведущими научными дисциплинами от безопасности до бизнеса, предпринимательства, правовых дисциплин и др.

В этой связи требуют решения вопросы организации и разработки концепции по формированию комплексного подхода по обеспечению кибербезопасности, включая разработку методологии и инструментария для практического внедрения, образовательный сегмент, возможности искусственного интеллекта, реализованные в отечественных аппаратно-программных средах [7].

ХАРАКТЕРИСТИКИ КИБЕРБЕЗОПАСНОСТИ

В эпоху активного использования возможностей Интернета мы так и не научились полной защите от кибермошенничества. В «Лаборатории Касперского» проанализировали статистику переходов по заблокированным фишинговым[1] ссылкам [4] и составили рейтинг ресурсов, которые подделывают чаще всего. На первом месте – мессенджеры (19%), второе место занимают почтовые сервисы и веб-порталы (18,5%), третьими в списке оказались онлайн-игры – 11%, банки – 10,5% и на пятом месте – онлайн-магазины с 8%[2]. Киберпреступность становится «бизнес-сообществом» со своими правилами и конкуренцией, оно постоянно совершенствуется для привлечения новых клиентов-преступников и, соответственно, денег. Разумеется, это не означает, что пользователям следует отказаться от онлайн-сервисов — кибербезопасность в постоянной готовности к новым и усовершенствованным старым угрозам, но в то же время мы должны серьезно относиться к этому вопросу, иначе однажды можем безнадежно отстать.

Кибербезопасность – это стратегия как превентивных, так и/или упреждающих действий. Она обеспечивает технологический рост и продвижение вперед, должна строиться на инновациях, так как надо научиться быть всегда на шаг впереди возможных действий второй стороны (противоборствующей). Реальности виртуального информационного пространства, которую нам «обеспечивает» всемирная паутина, существующие информационные методы и возможности в настоящее время пронизывают все стороны нашей жизни, полностью или частично определяют множество современных технологий, связанных с информационными процессами. Все элементы, с которыми мы работаем профессионально или в частном порядке в определенный момент времени, опираются или зависят от технологических достижений, которые облегчают и в то же время усложняют нашу жизнь, в то время как мы нуждаемся в постоянной и усиленной кибербезопасности наших данных, а также виртуального образа жизни [14].

Динамика дальнейшего развития кибервозможностей НАТО носит многовекторный характер и тенденцию развития многопрофильности кибероборонь Альянса. Надо понимать, что вместе с активным внедрением ИТ неизбежно будут расти и уязвимость защитных мер, и дополнительные расходы на оборону. Предусмотреть, изучить и предотвратить различные виды кибератак намного сложнее, чем реагирование на традиционные типы угроз [6].

В ответ на действия зарубежных поставщиков Президентом России принято решение о разви-

[1] **Фи́шинг** (от англ. fishing – рыбачить, выуживать) – разновидность попыток несанкционированного доступа, когда жертву провоцируют на разглашение информации, посылая ей фальсифицированное электронное письмо с приглашением посетить веб-сайт, который на первый взгляд связан с законным источником.

[2] Сайт: Реальное время. Киберпреступность: основные тренды и угрозы в 2024 году. [Электронный ресурс]. URL: https://realnoevremya.ru/articles/303048-kiberprestupnost-osnovnye-trendy-i-ugrozy-v-2024-godu (дата обращения: 29.02.2024).

тии программы импортозамещения и установлен срок перехода на отечественные средства защиты до 1 января 2025 года. В том числе вводится запрет на использование любого иностранного софта на объектах критической информационной инфраструктуры (КИИ) России[3].

Стратегически важна постоянная устойчивость безопасности. Безопасность как политика – это метод защиты. Среди прочего, она отражает политику правительства. В виртуальном мире благодаря кибербезопасности могут иметь место демократия, развитие, устойчивость и рост, инновации и предпринимательство.

Кибербезопасность – это одновременно стратегия и операционная основа, область оперативного потенциала, элемент междисциплинарного подхода, который подходит для всех уровней информационного управления: социально-политического, экономического, инженерного, информационно-предметного, юридического и ряда других, в контексте вопросов безопасности.

В то время как наблюдается активное развитие киберпространства в виде появления новых методов и способов несанкционированного проникновения в информационные системы, с оной стороны, а также средств защиты данных, с другой стороны, все еще нельзя говорить о едином подходе к формированию терминосистемы в этой области. До сих пор нет общепринятого определения этой сферы, в настоящее время для ее рассмотрения используется концепция «киберпространство». В табл. 1 представлен ряд определений, как на основе действующих стандартов, так и с учетом данных, например, Европейского агентства сетевой и информационной безопасности (ENISA) [18].

[3] Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001202203300001?index=2 (дата обращения: 29.02.2024).

Таким образом, кибербезопасность – это широкое понятие, и необходимо проводить различия между возможными типами кибератак. Киберпреступность, безусловно, является растущей сферой деятельности, поэтому необходимо принятие мер гражданского и правового характера. На этом этапе определяющей является роль органов управления и органов правосудия, а роль института НАТО здесь неуместна. Однако кибершпионаж – это та область, где решаемые задачи военными органами представляют интерес для противника, поэтому отраслевые сети и объекты соответствующих предприятий, научных центров хранят чрезвычайно важную и конфиденциальную информацию, которая может быть использована в политических и военных интересах многих заинтересованных стран, не являющихся членами НАТО. Кибертерроризм, кибервойна, кибердиверсии, а также возможные результаты этой деятельности представляют серьезную опасность для критической информационной инфраструктуры КВО (программное обеспечение, система управления и средства связи, которыми пользуются банки, госструктуры, предприятия топливно-энергетического комплекса и другие организации, повреждение информационных сетей которых может привести к серьезным последствиям для граждан и экономики). Силы Альянса участвовали в широком спектре конфликтов после окончания холодной войны, и кибероперации все чаще становятся частью этих конфликтов и элементом планов и сценариев действий. В табл. 2 представлены категории многомерных проблем, связанных с повышением кибербезопасности, и указаны области, в которых участники Североатлантического союза могут иметь основные интересы [13].

ИДЕИ СТАНДАРТИЗАЦИИ КИБЕРСФЕРЫ

Способность работать сообща в новых условиях безопасности на межгосударственном

Таблица 1

ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

ОСНОВНЫЕ ПОНЯТИЯ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ	ИСТОЧНИКИ
Кибербезопасность (киберзащита) – действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли или повреждения критических систем или информационных объектов. Кибербезопасность включает в себя понятия идентификации, аутентификации, отслеживаемости, авторизации, доступности и приватности	ГОСТ Р 56205–2014; (п. 3.2.36) [4]
Информационная безопасность – сохранение конфиденциальности, целостности и возможности доступа к информации	ГОСТ Р 57392–2017; (п. 2.11)
Безопасность информации [данных] определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, с несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые при применении информационной технологии	Р 50.1.056–2005; (п. 3.1.3)
Компьютерная безопасность – защита компьютерного аппаратного и программного обеспечения от случайного или предумышленного доступа, использования, модификации, уничтожения или разглашения. Также безопасность относится к персоналу, данным, коммуникационным связям и физической и логической защите компьютерных инсталляций	ГОСТ 33647–2015 (п. 3.5.10)
Киберпространство – это зависящий от времени набор материальных и нематериальных активов, которые хранят и/или передают электронную информацию	Kutlu F.B. [18]
Кибератака – всевозможные вредоносные действия, направленные на нарушение целостности, доступности и конфиденциальности информационных сетей, систем или непосредственно информации	Jasper S. [16]
Компрометация данных – нарушение безопасности, которое приводит к случайному или незаконному разрушению, потере, изменению, несанкционированному раскрытию или доступу к защищаемым данным, передаваемым, хранимым или иным образом обрабатываемым	ГОСТ Р ИСО/МЭК 27017–2021; (п. 3.1.2)

Таблица 2

КИБЕРБЕЗОПАСНОСТЬ В РАЗБИВКЕ ПО ЦЕЛЯМ, КАТЕГОРИЯМ И МОТИВАЦИИ

ЦЕЛИ КИБЕРАТАК	КИБЕРПРЕСТУПНОСТЬ (ПРЕСТУПНАЯ МОТИВАЦИЯ)	КИБЕРШПИОНАЖ (РАСШИРЕНИЕ ВОЗМОЖНОСТЕЙ ГОСУДАРСТВА)	КИБЕРТЕРРОРИЗМ (ПОЛИТИЧЕСКОЕ ПРИНУЖДЕНИЕ, ВЫЗЫВАЮЩЕЕ СТРАХ)	КИБЕРВОЙНА (УСИЛЕНИЕ ВОЕННЫХ ОПЕРАЦИЙ)
Частные лица	x			
Предприятия не из состава КИИ	x	x	x	x
Предприятия КИИ	x	x	x	x
Правительственные ведомства/объекты		x	x	x
Вооруженные силы/ силы обороны		x	x	x
Условные обозначения	Основная роль НАТО – ■; Периферийная роль НАТО – ■			

уровне важна, как никогда. Государствам необходимо использовать общий набор стандартов для торговли, информационного обмена, в сфере образования и в других областях. Этому способствуют существующие отечественные системы классификации и кодификации.

Стандартизация Североатлантического союза направлена на разработку и внедрение концепций, доктрин и процедуры для достижения и поддержания требуемых уровней совместимости, взаимозаменяемости и общности, необходимых для достижения интероперабельности.

Совместимость обеспечивает возможность встраиваться в информационную систему (НАТО) другого типа оборудования (в случае венгерских сил обороны с российским оборудованием) [20]. Взаимозаменяемость дает возможность обмена одного оборудования на другое. В ходе совместных операций страны могут обмениваться всеми типами ресурсов. Общность выражает состояние, при котором различные группы используют общие ресурсы или преследуют общие цели за счет реализации интеграции сил и средств, и начинается со стандартизации, результатом которой является более высокий уровень оперативной и информационной совместимости [1].

Защита организаций от киберугроз при одновременной демонстрации соответствия законам и стандартам рассматривается как чрезвычайно сложная задача из-за трудностей с выбором подходящего стандарта для использования. Более того, недостаток знаний о необходимых элементах, предлагаемых стандартом, а порой и отсутствие самого стандарта, приводит к проблеме определения начальной точки, с которой будет начата защита. Кроме того, многим организациям, компаниям не хватает опытного персонала в области кибербезопасности, поэтому им трудно внедрить стандартный подход или структуру кибербезопасности [19]. Недостаточная осведомленность общественности о применении кибербезопасности для защиты ИТ-активов, информации (цифровых данных), принадлежащих частным лицам или организациям, может стать причиной фактической потери информации.

Приведем анализ возможностей стандартизации в области кибербезопасности в сравнении с функционалом, реализованным в рамках отдельных пакетов или программ, антивирусных приложений, которые обобщим понятием «рамочная структура» (РС), представленным в табл. 3 [19].

Стандарты кибербезопасности – это наборы технических правил или практик, обычно используемых для защиты киберпространства или пользователей в организациях, имеющих подключение к Интернету. Целью внедрения стандартов кибербезопасности является повышение информационной безопасности, программного обеспечения, сетевых систем, инфраструктуры ИТ и другой КВО. Стандарт также может определять функциональные требования и гарантии в процессах, системах, производственных средах, активах и технологиях.

Киберсреда включает в себя самих пользователей, сетевую инфраструктуру, аппаратное и программное обеспечение, процессы и сервисы, локальную, облачную или транзитную информацию, включая системные носители информации, которые могут быть подключены прямо или косвенно к сети Интернет. Основной целью является снижение риска, включая предотвращение или смягчение последствий кибератак.

УСТОЙЧИВОСТЬ КАК МЕТОДОЛОГИЯ: СТРАТЕГИЧЕСКАЯ ЦЕЛЬ

Устойчивость представляет собой важное свойство большинства сложных технических систем, характеризующее их структуру (техническую, функциональную, программно-математическую) [2]. Устойчивость выступает в роли целевого фактора, ориентированного на безопасность, а в рассматриваемой постановке – на кибербезопасность в приложениях программе РС.

Концепция устойчивости признает стремление к обеспечению готовности для противодей-

Таблица 3

СРАВНЕНИЕ ПОДХОДОВ В СТАНДАРТИЗАЦИИ И В РС

СТАНДАРТЫ	РАМОЧНЫЕ СТРУКТУРЫ
1. Добровольные документы, определяющие спецификации, процедуры и руководящие принципы для обеспечения безопасности, согласованности и надежности продуктов, услуг и систем. 2. Правила или документы, составленные на основе общего соглашения и одобренные юридическим лицом, которые определяют общее использование, регулирование, регламентацию или качество деятельности (масштаб предприятия). 3. Может быть разработан компанией (стандарт организации) или государством в виде стандарта. 4. Должен соблюдаться организацией-исполнителем в соответствии с правовыми или нормативными положениями. 5. Может использоваться вместе с другими стандартами для дополнения и усиления отдельных требований. 6. Существуют стандарты для всех типов предприятий и государственных организаций («открытые»); другие («закрытые»), специфичны для определенных отраслей или предприятий. 7. Определяет, что должно быть сделано для соответствия стандарту.	Общее руководство, которое может быть принято предприятиями / фирмами/ учреждениями, охватывающее многие компоненты или предметные области, но не определяющее шаги, которые необходимо предпринять: ■ предоставляет только общее описание в качестве основы для создания чего-либо или достижения общей цели; ■ используется для подведения итогов достижения целей, описания сферы охвата, руководства внедрением и оценкой, а также определения стандартов качества, которые должны быть достигнуты.

ствия возможной интегративной составляющей возникающих кризисных явлений. Она рассматривается как инновационная процедура и инструмент политики стратегического управления. Именно на стратегическом уровне важен переход от РС – подхода к стандартизации процессов взаимодействия. В оборонном секторе, когда силы развертываются, им нужны гибкие и эффективные средства противодействия угрозам. Работая в сфере кибербезопасности, они нуждаются в гибкости в оперативных действиях, ориентированных на сетевые технологии, мониторинг и достоверные информационные потоки.

Стратегическая устойчивость в области кибербезопасности требует гибкой адаптации на уровне технологий, аппаратно-программных средств, постоянно расширяя инструменты сближения, интеграции и инноваций.

Последнее реализуется в концепции «интеллектуальной обороны» (или смарт-обороны), которая представляет собой измененный взгляд, лучшую стандартизацию, возможность для обновления информационного взаимодействия на всех уровнях, от технологического до организационного, реализуя новые критически важные возможности. В частности, концепция «Умная оборона» рассматривается в контексте сотрудничества НАТО с Европейским союзом по объединению и совместному использованию ресурсов (природных, образовательных, производственных мощностей и др.).

На рис. 1 показаны цели киберустойчивости (вверху) и связанные с ними задачи (внизу) из РС (отдельных приложений) в области киберустойчивости [17].

1 Планирование/подготовка

На данном этапе киберустойчивость использует хорошо известные компоненты архитектуры, отношения и структуры с избыточностью, сегментацией, мониторингом, координацией и так далее. Понимание (осознание), подготовка и предупреждение (прогноз) обеспечивают устойчивость на уровне применяемых программных платформ и информационно-коммуникацион-

ных технологий для взаимосвязи между операциями (оперативными процедурами) и этапами. Разрешать динамическую реконфигурацию и перераспределение ресурсов, используя динамическое представление и механизмы контроля целостности данных.

2 Усвоение

Продолжение операций или обеспечение выполнения миссии может потребовать непредвиденных изменений базовой архитектуры системы в зависимости от того, что вышло из строя в результате кибератаки. Однако изменений могут потребовать не только технические системы, но также операционные процедуры и способ обмена информацией. Следствием этого может быть необходимость альтернативной коммуникации и обработки данных наряду с изменением операционных процедур, что приводит к различным корпоративным архитектурам по горизонтали и вертикали, которые заранее не планировались, а выполняются по факту.

3 Восстановление

Конечное состояние этапа восстановления обычно поддерживается архитектурой. Однако переход из любого незапланированного состояния в восстановленное при сохранении непрерывности работы требует достаточно полного анализа вариантов переключений на этапе планирования, например, в ходе имитационного моделирования. Обеспечение свойств гибкости и интероперабельности позволит перепрофилировать киберресурсы для резервирования мощностей и безопасного перехода на другой ресурс.

4 Адаптация

Этап перепроектирования часто является наиболее понятной частью процесса создания архитектуры киберустойчивости, поскольку физически понятно, как можно обеспечить реструктуризацию или реконфигурацию на основе предыдущих этапов, технических требований, а также возможностей применений новых технологий для повышения устойчивости с учетом модульности и гибкости управления киберресурсами, перемещая и обновляя их.

ГИБРИДНЫЕ ПОДХОДЫ В ФОРМАТЕ «СДЕРЖИВАНИЯ»

В западных источниках все активнее даются прогнозы на использование кибероружия в будущих военных столкновениях [15, 16]. Эти наступательные кибернетические возможности в руках

Рис. 1. СОГЛАСОВАНИЕ ЦЕЛЕЙ И ЗАДАЧ ОБЕСПЕЧЕНИЯ КИБЕРУСТОЙЧИВОСТИ НА ТЕОРЕТИЧЕСКОМ И ИНЖЕНЕРНО-ТЕХНИЧЕСКОМ УРОВНЯХ

противников представляют значительную угрозу вооруженным силам и КВО для каждой из сторон конфликта. Североатлантический союз признает, что кибератаки (как гибридные угрозы) могут быть такими же разрушительными, как и обычные военные действия. Вредоносные кибератаки, нацеленные на управляющие вычислительные комплексы КВО, могут быть не менее опасными, чем угрозы физического характера, и могут привести к взрывам, ядерным авариям, отключениям электроэнергии или финансовым кризисам. По заявлениям представителей НАТО, «всего за несколько минут одна кибератака может нанести ущерб экономике на миллиарды долларов, парализовать КИИ и подорвать военный потенциал» [15].

В рассуждениях западных военных аналитиков прослеживается идея необходимости развития наступательных кибервозможностей и интеграции их в военные операции. Для того, чтобы избежать перерастания в тотальную войну во время «тумана войны»[4], союзники по Альянсу должны согласовать список гибких средств «сдерживания»[5], которые позволят постепенно наращивать давление в киберпространстве для ограничения масштаба и интенсивности возможных конфликтов, хотя нет гарантий, что эти меры могут быть использованы в качестве превентивных. Гибкие варианты «сдерживания» НАТО в киберпространстве могли бы включать (см. рис. 2):

❶ повышение готовности сил и средств посредством киберобразования, тренингов и учений;

❷ развертывание групп «быстрого реагирования» в киберпространстве для проведения оборонительных кибероперации и защиты КВО;

❸ повышение информированности общественности о вредоносной кибердеятельности и потенциальном конфликте в киберпространстве;

❹ принятие мер по взаимной поддержке союзных государств Альянса;

❺ расширение мер по информационному взаимодействию в киберпространстве;

❻ официальные заявления о нарушениях международного права в киберпространстве;

[4] **Туман войны (туман неизвестности)** – военный термин, обозначающий отсутствие достоверной информации о текущей обстановке на поле боя.

[5] Кавычки автора.

Рис. 2. ПРЕДЛАГАЕМЫЕ НАТО ГИБРИДНЫЕ ВАРИАНТЫ СДЕРЖИВАНИЯ В КИБЕРПРОСТРАНСТВЕ [15]

❼ приведение в готовность и развертывание сил для проведения наступательных кибероперaций;

❽ введение киберсанкций;

❾ проведение наступательных кибероперaций для достижения эффекта A2/AD (препятствие доступу/закрытие зоны – Anti-Access/Area Denial) в киберпространстве;

❿ приведение комплекса мер в соответствие с Договором Альянса в полной мере;

⓫ проведение наступательных кибероперaций совместно с другими маневренными силами во всем оперативном пространстве.

При всей важности вопросов кибербезопасности следует отметить, что в реальной жизни существует множество факторов, из-за которых системы АСУ технологическими процессами могут выйти из строя не только по причинам вредоносного программного обеспечения, хакерской целенаправленной атаки или мошенничества. Иногда это просто проявление халатности, допущения ошибки, недостатка компетенции или недобросовестного действия (бездействия) со стороны персонала [5]. Поэтому к критериям защищенности нужно отнести не только защиту от внешних или случайных атак, но и инструменты предупреждения и предотвращения некорректных или ошибочных действий со стороны собственных сотрудников. Вот почему актуальным становится социальный запрос о необходимости ведения образовательной деятельности [10] среди населения по совершенствованию культуры информационной безопасности.

ВЫВОДЫ И ПРЕДЛОЖЕНИЯ

1 Вместе с тем внедрение высоких технологий связано с появлением новых технологических рисков, появление которых необходимо прогнозировать, к ним следует готовиться заранее и разрабатывать соответствующие методы управления, чтобы минимизировать их степень воздействия или, по возможности, купировать. Сложность управления рисками обусловлена тем, что риски внедрения новых технологий очень разнообразны: это и появление новых вирусных программ, угрозы внешнего управления, исчезновения приватности, тайная слежка, утечка персональных данных, контроль рынка и многое другое.

2 Ввиду того, что при рассмотрении вопросов кибербезопасности на карту ставится безопасность политическая, технологическая, социальная, то ряд приложений и конкретные направления организационной деятельности следует рассматривать через призму их решения военными зарубежными альянсами. Неслучайна же военная направленность применяемых терминов в этой сфере: кибератака, кибершпионаж, кибертерроризм, кибервойна. Операции кибервойн могут включать действия шпионажа, взлома, дестабилизации компьютерных систем и распространения нежелательного программного обеспечения. Кибервойны часто также направлены на создание хаоса и паники среди населения противника или нарушение жизнедеятельности страны.

3 Киберзащита может использоваться в качестве основной политики интеллектуальной обороны. Скоординированный уровень тактического военного и гражданского потенциала и развертывания потенциала в тактических симметричных или асимметричных операциях. Эта статья предоставляет читателю обновленную информацию о политике киберзащиты, «умной обороне» и Североатлантическом альянсе. Это важная тема исследования, которая может оказать влияние на практике. Эта статья является аналитической и экзаменационной. В ней рассматриваются «извлеченные уроки» на сегодняшний день. В нем рекомендуются вопросы для будущего управления потенциалом, администрирования и финансовых затрат на киберзащиту в стратегических сетевых операциях.

Список использованных источников и литературы

1. Бурый А. Состояние и тенденции развития стандартизации государств – членов НАТО // Военная стандартизация. 2023. № 2. С. 46–53.
2. Бурый А.С. Введение в теорию синтеза отказоустойчивых многозвенных систем переработки навигационно-баллистической информации. – М.: ВА РВСН им. Петра Великого, 1999. – 299 с.
3. Валиахметова Г.Н., Цуканов Л.В. «Сумма всех ресурсов страны»: специфика израильского подхода к обеспечению национальной кибербезопасности // Уральское востоковедение. 2021. № 11. С. 23–34.
4. ГОСТ Р 56205–2014 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели. (Введ. 2016-01-01). – М.: Стандартинформ, 2020. – 76 с.
5. Духвалов А.П. Кибератаки на критически важные объекты – вероятная причина катастроф // Вопросы кибербезопасности. 2014. № 3(4). С. 50–53.
6. Курылев К.П., Цаканян В.Т. Цифровая зависимость НАТО // Вестник Московского государственного областного университета. Серия: История и политические науки. 2018. № 1. С. 45–53.
7. Малаев А.Х. Применение цифровых технологий и искусственного интеллекта при предупреждении экстремистских и террористических преступлений // Пробелы в российском законодательстве. 2023. Т. 16. №4. С. 263–267.
8. Малюк А.А., Полянская О.Ю. Зарубежный опыт формирования в обществе культуры информационной безопасности // Безопасность информационных технологий. 2016. Т. 23, № 4. С. 25–37.
9. Манойло А.В. Современные стратегии кибербезопасности и кибероборонны НАТО // Актуальные проблемы Европы. 2020. № 3(107). С. 160–184.
10. Махалин В.Н., Махалина О.М. Управление вызовами и угрозами в цифровой экономике России // Управление. 2018. Т. 6, № 2. С. 57–60.
11. Лебедь С. В. Инновационные технологии в сфере кибербезопасности // Современные информационные технологии и ИТ-образование. 2022. Т. 18, № 2. С. 383–390.
12. Плеханова О.А. Безопасность киберфизических систем на предприятиях // Экономический вестник. 2023. Т. 2, № 2. С. 17–21.
13. Burton J. NATO's cyber defence: strategic challenges and institutional adaptation // Defence Studies. 2015. Т. 15, № 4. С. 297–319.
14. Efthymiopoulos M.P. A cyber-security framework for development, defense and innovation at NATO // Journal of Innovation and Entrepreneurship. 2019. Т. 8, № 1.
15. Iftimie I.A. NATO's needed offensive cyber capabilities // NATO Defense College. 2020. URL: http://www.jstor.org/stable/resrep25100 (дата обращения: 29.02.2024).
16. Jasper S. Strategic cyber deterrence: The active cyber defence option. Rowman & Littlefield. 2017.
17. Kott A. et al. Approaches to enhancing cyber resilience: Report of the north atlantic treaty organization (NATO) workshop IST-153 // arXiv preprint arXiv:1804.07651. 2018.
18. Kutlu F.B. A New Field Between Two Old Allies: Cybersecurity Approaches of EU and NATO (2016–2020) // Journal of Diplomatic Research. 2023. Т. 5. № 1. С. 24–41.
19. Syafrizal M., Selamat S.R., Zakaria N.A. Analysis of cybersecurity standard and framework components // International Journal of Communication Networks and Information Security. 2020. Т. 12, № 3. С. 417–432.

АНДРЕЙ СУХОВ,
д-р техн. наук, профессор, ведущий научный сотрудник ФКУ НПО «СТиС» МВД России, гл. спец. ФГБУ «Институт стандартизации»
СЕРГЕЙ ПУЗИЙЧУК,
начальник центра ФКУ НПО «СТиС» МВД России

ИНФОРМАЦИОННЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ РАДИОПРОТИВОДЕЙСТВИЯ БЕСПИЛОТНЫМ ВОЗДУШНЫМ СУДАМ

В статье представлен анализ эффективности радиоэлектронного противодействия несанкционированным беспилотным воздушным судам, основанный на оценке информационного ресурса беспилотного воздушного судна в терминах энтропии покрытия. Информационный ресурс рассматривается как энтропия покрытия по радиоэлектронным показателям беспилотных воздушных судов в условиях внешних радиоэлектронных воздействий. Для радиоэлектронного подавления задаются радиолинии управления беспилотными воздушными судами, радиолинии навигационных определений по космическим навигационным системам и радиолинии передачи телеметрии. Энтропия покрытия при этом с комплексных целевых позиций позволяет дать информационную оценку эффективности принятых мер по противодействию беспилотным воздушным судам. В целях получения количественных оценок потребовалось провести оценку бюджета радиоканалов, связанных с беспилотными воздушными судами.

ЗАДАЧИ ПРОТИВОДЕЙСТВИЯ БЕСПИЛОТНЫМ ВОЗДУШНЫМ СУДАМ

В настоящее время во всех сторонах активной дельности человечества, связанной с применением технических средств, все большее применение находят беспилотные воздушные суда (БВС), позволяющие значительно облегчить решение поставленных технических задач, расширить круг решаемых технических проблем. Широкое применение БВС находят в военной области, но и в других сферах человеческой деятельности их применение становится все более востребованным, а в ряде случаев просто необходимым [1–3].

К распространенным задачам гражданских БВС можно отнести:

- ведение наблюдения за объектами – аэрофотографическая, тепловая инфракрасная, радиолокационная, многозональная и другие виды съемки;
- геофизическая съемка – аэромагнитная, аэ-

рорадиометрическая, аэроспектрометрическая – в результате выполнения которых получают цифровую информацию об исследуемых объектах;
- транспортировка и доставка грузов и средств в заданный район;
- ретрансляция данных между удаленными абонентами сетей связи.

Решение задач, поставленных БВС, осуществляется оператором при их дистанционном управлении или путем автономных действий по заранее заложенной программе.

Но с использованием БВС решаются также и задачи, которые не могут быть согласованы с действующим законодательством. При этом БВС могут нарушать установленные правила полетов воздушных судов и не иметь определяемой законами государства регистрации. Также такие БВС могут являться угрозой жизни, здоровья и имущества граждан в том числе над местами проведения публичных (массовых) мероприятий. Эти БВС определим как несанкционированные БВС. В Приказе МВД России от 30 апреля 2020 г. № 252[1] указывается, что в этих случаях пресечение нахождения БВС в воздушном пространстве осуществляется посредством подавления или преобразования сигналов дистанционного управления БВС, воздействия на их пульты управления, а также повреждения или уничтожения БВС и приводится порядок действий должностных лиц органов внутренних дел.

Для выполнения поставленных БВС задач создаются наземные технические средства передачи-получения данных (НТС ППД), используемые для управления полетом и обмена данными о параметрах полета, служебной информацией и информацией о полезной нагрузке такого или таких ВС, и канал связи со службой управления воздушным движением [2, 4].

Наземная станция управления (НСУ) системы управления (СУ) БВС включает в свой состав человека-оператора и НТС ППД, основу которых составляют планшетный компьютер или ноутбук, приемопередатчик (ПП) и антенно-фидерное устройство (АФУ). Математическое обеспечение НТС ППД реализуется программным обеспечением для планирования полетного задания и отображения хода его выполнения. Сигнально-кодовые конструкции, формируемые в ПП, обеспечивают необходимую помехозащищенность радиоканалов.

Полетное задание может составляться автоматически по заданному контуру площадного объекта или по узловым точкам линейного объекта, может формироваться человеком-оператором для решения конкретных задач. Существует возможность проектирования полетных маршрутов, исходя из необходимой высоты полета и требуемого разрешения фотоснимков на местности. Для ряда задач и соответствующих типов БВС используется цифровая модель местности. Оператор во время выполнения полета БВС имеет возможность оперативно выбрать необходимый район посадки или оперативно посадить беспилотник с «красной» кнопки наземной системы управления. По команде человека-оператора (внешнего пилота) могут быть заданы вспомогательные операции для БВС.

В состав БВС для обеспечения навигации и обеспечения полета может быть включен автопилот, который должен управлять маршрутом движения воздушного судна и выполнением специальных операций, например съемкой местности или объектов с заданным межкадровым временным интервалом.

Автопилот должен определять координаты БВС, как правило, с использованием гло-

[1] Приказ МВД России от 30 апреля 2020 г. № 252 «Об утверждении Порядка принятия решения о пресечении нахождения беспилотных воздушных судов в воздушном пространстве в целях защиты жизни, здоровья и имущества граждан над местом проведения публичного (массового) мероприятия и прилегающей к нему территории, проведения неотложных следственных действий и оперативно-разыскных мероприятий и Перечня должностных лиц, уполномоченных на принятие такого решения».

бальных навигационных спутниковых систем (ГНСС) или осуществлять ориентирование в пространстве с использованием инерциальных датчиков. Требуемая точность определения координат зависит от технического задания на решаемые БВС задачи.

Полезная информация, получаемая БВС, данные телеметрии о текущем состоянии бортовой аппаратуры, координаты и результаты по решаемым в ходе полета задачам передаются с бортового ПП на НТС ППД.

Противодействие БВС осуществляется с целью недопущения противоправного применения БВС, недопущения решения БВС противоправных задач. При этом в условиях, не связанных с ведением боевых действий, применение зенитных комплексов огневого поражения БВС не является оправданным. Вполне обоснованными способами противодействия БВС являются способы радиоэлектронного подавления радиоканалов БВС, таких, как навигационные радиоканалы, каналы радиоуправления, телеметрии, передачи целевой информации. Средства РЭП могут создавать шумовые и имитационные помехи на БВС.

Схема воздействия комплекса радиоэлектронного противодействия (РЭП) на БВС показана на рис. 1.

На рис. 1 использованы следующие обозначения:

КА1, КА2, … KAN – космические аппараты группировки ГНСС, используемые для навигационных определений;

$S_{упр}$ – линия управления и контроля с НСУ на БВС;

$S_{св}$ – линия связи БВС с НСУ;

$S_{нав}$ – сигналы с КА ГНСС, образующие навигационное поле;

РЭП – система радиоэлектронного противодействия;

$I_{БВС}$ – помехи от системы РЭП на БВС;

$I_{НСУ}$ – помехи от системы РЭП на НСУ

РАДИОЭЛЕКТРОННЫЕ ПОКАЗАТЕЛИ БВС, ОПРЕДЕЛЯЮЩИЕ УСТОЙЧИВОСТЬ К РАДИОЭЛЕКТРОННОМУ ПОДАВЛЕНИЮ

Как правило, БВС используют радиоканалы управления и контроля, радиоканалы передачи полезной информации и радиоканалы навигации СНС.

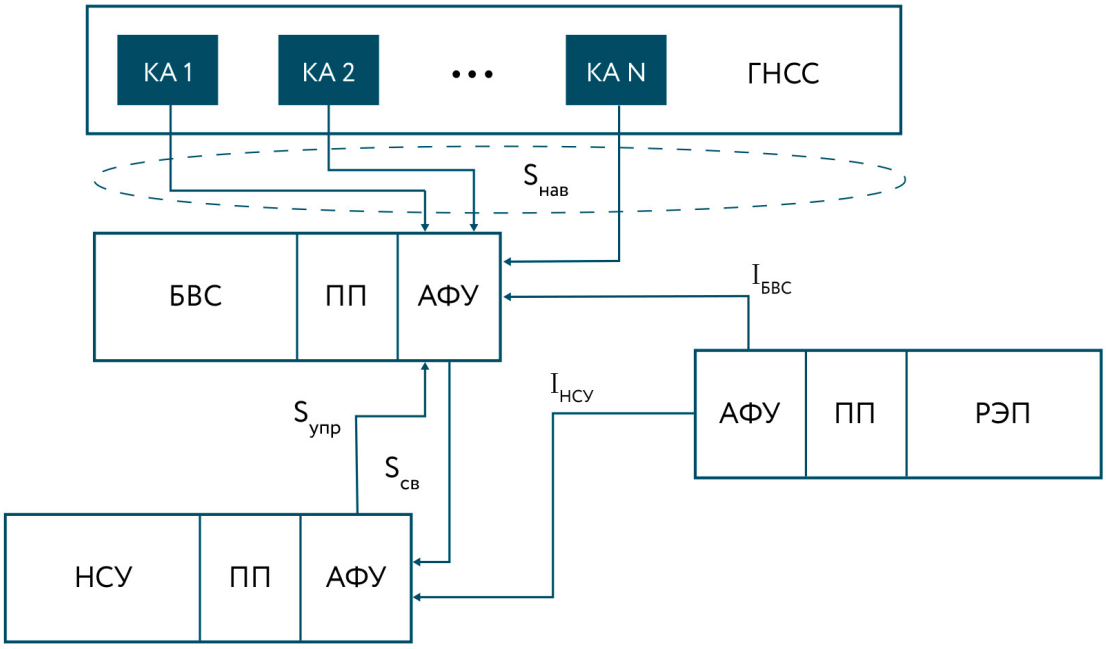


Рис. 1. Схема воздействия комплекса радиоэлектронного противодействия на БВС

ЦВ целях организации РЭП требуется задать диапазоны характеристик БВС, определяющие энергетические характеристики радиоканалов. Поскольку в данной статье не рассматриваются беспилотные летательные аппараты военного назначения, то основное внимание уделим тем характеристикам и их значениям, которые могут ожидаться у БВС, используемым в условиях мирного времени.

Классификация БВС приведена в ГОСТ Р 57258–2016[2]. В частности рассматриваемых в статье объектов вводятся следующие определения:

3.2.1 воздушное судно (aircraft): летательный аппарат, поддерживаемый в атмосфере за счет его взаимодействия с воздухом, за исключением случаев взаимодействия с воздухом, отраженным от поверхности земли или воды.

3.2.6 легкое дистанционно пилотируемое воздушное судно (light remotely piloted aircraft): дистанционно пилотируемое воздушное судно с взлетной массой менее 150 кг.

3.2.7 малое беспилотное воздушное судно (small unmanned aircraft): беспилотное дистанционно пилотируемое воздушное судно с взлетной массой менее 30 кг».

Сведения по существующим видам БВС широко распространены [5, 6]. В табл. 1 приведена классификация БАС, разработанная Международной ассоциацией беспилотных систем (AUVSI).

Диапазон значений технических характеристик, достаточно распространенных БВС, приведен в табл. 2.

Для средств РЭП необходимо определить диапазоны частот и параметры сигналов радиоканалов БВС для радиоподавления.

Характеристики радиосигналов ГНСС, создающих навигационное поле, приведены в табл. 3 [7].

Для приема сигналов от ГНСС могут использоваться антенны с коэффициентом усиления от 0 до 3 дБи, то есть либо всенаправленные антенны, либо антенны с полусферической диаграммой направленности.

Для приема-передачи радиосигналов по другим радиоканалам могут быть использованы диапазоны радиочастот, предназначенные в соответствии с таблицей распределения полос радиочастот в РФ[3] для воздушной подвижной (OR) службы радиосвязи (ВПРС), предназначенной для связи, в том числе связи, касающейся координации полетов главным образом вне национальных или международных гражданских воздушных трасс.

Для воздушной подвижной (OR) службы радиосвязи на частотах от 3 МГц до 144 МГц определен 21 диапазон. Но в этих диапазонах можно передавать только узкополосные сигналы. На частотах, начиная со 144 МГц и выше, уже можно обеспечить необходимую скорость передачи информации, то есть можно передавать и видеоинформацию.

Диапазон частот 144–146 МГц выделен ВПРС для РЭС любого назначения («СИ» – полоса радиочастот совместного пользования), а диапазон частот 146–148 МГц выделен ВПРС для «ПР» – полоса радиочастот преимущественного пользования РЭС, предназначенными для нужд государственного управления, в том числе президентской связи, правительственной связи, нужд обороны страны, безопасности государства и обеспечения.

[2] ГОСТ Р 57258–2016 Системы беспилотные авиационные. Термины и определения.

[3] Постановление Правительства Российской Федерации от 18 сентября 2019 г. № 1203-47. «Об утверждении Таблицы распределения полос радиочастот между радиослужбами Российской Федерации и признании утратившими силу некоторых постановлений Правительства Российской Федерации».

Таблица 1

ЗНАЧЕНИЯ ХАРАКТЕРИСТИК БВС, ОПРЕДЕЛЯЮЩИХ ЭНЕРГЕТИКУ РАДИОЛИНИЙ ДЛЯ РЭП

КАТЕГОРИЯ БВС	РАДИУС ДЕЙСТВИЯ, (км)	ВЫСОТА ПОЛЕТА (м)	ВРЕМЯ ПОЛЕТА (ЧАСЫ)	МАКСИМАЛЬНЫЙ ВЗЛЕТНЫЙ ВЕС MTOW (кг)
Nano	<1	100	<1	<0,025
Micro	<10	250	1	<5
Mini	<10	150 to 300	<2	<25
Close Range	10 to 30	3 000	2 … 4	150
Short Range	30 to 70	3 000	4 … 6	200
Medium Range	70 to 200	5 000	6 … 10	1 250
Medium Range Endurance	>500	8 000	10 … 18	1 250
Low Altitude Deep Penetration	>250	50 … 9 000	0,5 … 1	350
Low Altitude Long Endurance	>500	3 000	>24	<25
Medium Altitude Long Endurance	>500	14 000	24 … 48	1 500
High Altitude Long Endurance	>2000	20 000	24 … 48	5 000
Stratospheric	>2000	>20 000	>48	2 500
Exo-Stratospheric	>2000	>30 500	>48	2 500

Таблица 2

ДИАПАЗОН ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК БВС

ТЕХНИЧЕСКАЯ ХАРАКТЕРИСТИКА	МИНИМАЛЬНО УЧИТЫВАЕМЫЕ ЗНАЧЕНИЯ	МАКСИМАЛЬНО УЧИТЫВАЕМЫЕ ЗНАЧЕНИЯ
Высота полета, м	70–150	5000
Радиус применения, км	0,5	100/300*
Максимальная продолжительность полета, ч	0,5	4
Крейсерская скорость, м/с	10	100
ГНСС	ГЛОНАСС (Россия), GPS/NAVSTAR (США), Beidou (Китай), Galileo (ЕС)	

* Радиус применения (с БВС-ретранслятором).

Таблица 3

ДИАПАЗОНОВ ЧАСТОТ СПУТНИКОВЫХ СИСТЕМ СВЯЗИ

ГНСС	НЕСУЩИЕ ЧАСТОТЫ, МГц	ПОЛОСА СИГНАЛА, МГц	МОЩНОСТЬ СИГНАЛА У ПОВЕРХНОСТИ ЗЕМЛИ, дБВт
GPS	1575,42; 1227,6; 1176,45	2,046 … 25,5	157,0–167,5
ГЛОНАСС	1602 + k · 0,5625 k = -7 … +6; 1601,995; 1248,06; 1246 + k · 0,4375 k = -7 … +6; 1202,025	1,022 … 20,46	161–161,5
Galileo	1575,42; 1278,75; 1207,14; 1176,45	4,092 … 30,7	158–170,4
Beidou	1575,42; 1561,098; 1268,52; 1207,14; 1176,45	4,092 … 32,7	156,9–169,4

Таблица 4

ОСНОВНЫЕ ПОКАЗАТЕЛИ ОТЕЧЕСТВЕННЫХ СРЕДСТВ РЭП

СРЕДСТВО РЭП	ДИАПАЗОНЫ РАДИОЧАСТОТ	МОЩНОСТЬ ПЕРЕДАТЧИКА, ЭИМ*, Вт	ДАЛЬНОСТЬ ДЕЙСТВИЯ, км
Переносной комплекс противодействия БВС «Купол-ПРО»	Каналы связи, управления и навигационного обеспечения БВС	80*	2
Переносной комплекс противодействия БВС «Луч-ПРО»	Одновременное воздействие на каналы связи, управления и навигационного обеспечения БВС	—	4
Объектовый комплекс радиоэлектронного противодействия БВС «Таран-ПРО»	433 МГц ISM; 915 МГц ISM; 1,2 ГГц; 1,5 ГГц ISM; 2,4 ГГц ISM; 5,8 ГГц ISM / WiFi – Каналов GPS, ГЛОНАСС, Галилео (L5, E5ab, L1, E1, G1, G3), Beidou		2,7
Многофункциональный комплекс противодействия беспилотным летательным комплексам «Сапсан-Бекас»	В диапазоне работы средств связи и управления БВС	100	4
Стационарный комплекс противодействия БВС «Рубеж-Автоматика»	Частотные каналы связи, управления и навигационного обеспечения	–	4
Транспортируемый комплекс противодействия БВС «Бастион-Автоматика»	Частотные каналы спутниковой навигации, связи и управления		2
Персональный комплекс борьбы с дронами	1575; 2400–2480 МГц (настраивается в диапазоне от 400 до 2700 МГц)	20	2
Станция борьбы с радиоуправляемыми авиационными моделями	225–510, 800–900, 1100–1800, 2200–2500, 4400–5850 МГц	50	5
Ручной комплекс борьбы с беспилотными летательными комплексами «Гарпун-1»	Диапазоны частот каналов управления и навигации БВС (GPS / ГЛОНАСС / Beidou), 1600–2400, 5725–5875.	–	Дальность действия ограничена дальностью визуального контроля БВС.
Ручной комплекс борьбы с беспилотными летательными комплексами «Гарпун-2М» – многоканальный постановщик помех	433 МГц (430–450 МГц); 868 МГц (860–873 МГц); 900 МГц (902–928 МГц); 1200 МГц (1166–1281 МГц); 1,57542 / 1,602 ГГц; 2,4 ГГц (2,4–2,484 ГГц); 5,2 ГГц (5,15–5,35 ГГц); 5,8 ГГц (5,725–5,875 ГГц).	–	1,5
Комплекс обнаружения и защиты от беспилотных летательных аппаратов «Стриж-3»	433 МГц; 868МГц; 915 МГц; 1600 МГц; 2400 МГц; 5800 МГц	5	1,5
Мобильный комплекс обнаружения и защиты от беспилотных летательных комплексов «Скворец»	433 МГц; 868 МГц; 900 МГц; 1,6 ГГц; 2,4 ГГц; 5,8 ГГц	5	1,5
Средство противодействия БВС «REX-2»	430 МГц, 900 МГц, 1,3 ГГц, 1,8 ГГц, 2,4 ГГц, 2,6 ГГц, 4 ГГц,	–	2
Система «Репеллент»	от 200 до 6000 МГц	канала передачи данных от 300 до 500 Вт;подсистемы канала управления и телеметрии от 500 до 1000 Вт	10 … 30

* ЭИМ – эффективная излучаемая мощность.

В соответствии с примечанием 127 к таблице радиочастот РФ[4], для СУ БВС могут использоваться полосы радиочастот 230–299,3 МГц, 308,4–328,6 МГц и 344,4–390 МГц, которые преимущественно используются воздушной подвижной службой (OR).

Также БВС могут использовать радиодиапазоны, выделенные для беспроводной связи (Wi-Fi, Bluetooth, ISM), но в этих диапазонах

[4] Там же.

возможна организация связи только на небольших расстояниях из-за низкой мощности передатчика, поскольку эти средства, как правило, работают в диапазонах частот, которые выделены и на первичной основе, и на вторичной основе другим службам, и создание радиопомех РЭС этим службам недопустимо.

Основные показатели средств РЭП приведены в табл. 4 [8].

Для управления специальными малыми БВС (например, такими как RQ-7B Shadow 200, RQ-11B Raven, RQ-16T-Hawk и др.), как правило, организуется радиоканалы управления в режиме прямой видимости с НСУ или с ретранслятором:

- каналы в L (1,4–1,85 ГГц), S (2,2–2,5 ГГц), C (4,4–5,85 ГГц), и Ku (15,15–15,35 / 14,4–14,83 ГГц) диапазонах – основные каналы управления;
- в УКВ диапазоне (220–400 МГц) – резервные каналы управления;
- спутниковый канал (как правило используется низкоорбитальная спутниковая система связи Iridium обеспечивающая возможность использованиям небольших антенн) L-диапазона (1,616–1,6265 ГГц) – резервный канал управления, устанавливаемый опционально на отдельных БВС.

Ширина полос частот каналов СУ БВС [8]:

- канал «вверх» в диапазонах L, S, C и Ku: в режиме фиксированной частоты – 300–700 кГц; в режиме шумоподобного сигнала (ШПС) – 0,7–28 МГц;
- канал «вниз» в диапазонах L, S, C и Ku: 3–20 МГц;
- каналы «вверх»/ «вниз» в УКВ диапазоне: 25 кГц.

Чувствительность приемников находится в пределах: 127–134 дБВт.

Скорости передачи данных в СУ БВС:

- до 20 кбит/с – в линии «вверх»; 200 кбит/с – в линии «вниз» (при передаче только телеметрии); 1,6–12 Мбит/с – в линии «вниз» в диапазонах L, S, C и Ku (при передаче телеметрии совместно с данными от оптико-электронных систем при визуальном управлении оператором);
- 2,4–16 кбит/с в линиях «вверх»/«вниз» в УКВ диапазоне;
- до 2,4 кбит/с в линиях «вверх»/«вниз» по спутниковой линии L диапазона (для спутниковой системы связи Iridium).
- в диапазонах L, C, S, Ku в каналах «вверх»/«вниз»: 5–15 Вт;
- в УКВ диапазоне в каналах «вверх»/ «вниз»: 15–25 Вт.

Для связи с БВС используются типы модуляции сигналов: BPSK, QPSK (DQPSK, SOQPSK), 2FSK, GMSK. Возможно использование режима сигналов с псевдослучайной перестройкой рабочей частоты (ППРЧ) в пределах разрешенной к использованию полосы частот в диапазонах S, C и Ku. С целью обеспечения необходимой помехоустойчивости применяется помехоустойчивое кодирование сигналов. Скорости кода R =1/2, 2/3, 3/4.

Обобщая приведенный материал и с учетом [8] можно определить требования к основным характеристикам систем РЭП:

1. Требования по радиочастотам:
   - диапазон частот, в котором ведется подавление: 200–6000 МГц;
   - подавление выделенных полос частот:

а) частоты типовых каналов нелицензированных средств радиосвязи: 20–80, 135–174, 400–470 МГц;

б) частоты типовых каналов авиационной радиосвязи в диапазоне 220–400 МГц;

в) частоты типовых каналов коммерческих систем связи: 430–460, 860–880, 902–928 МГц, CDMA800 (850–894 МГц), GSM900 (890–915, 935–960 МГц), GSM1800 (1710–1880 МГц), 3G (2110–2170 МГц), 4G (725–770, 780–960, 925–960 МГц; 1,7–2,2, 2,5–2,7 ГГц), Wi-Fi (2,4–2,5,

4,9–6,425 ГГц);

г) частоты каналов «вниз» спутниковых систем связи (ССС) L-диапазона: Инмарсат (1518–1660,5 МГц), Иридиум (1616¬1626,5 МГц);

д) частоты каналов ГНСС: GPS (L1 – 1575,42 МГц / L2 – 1227,6 МГц / L5 – 1176,45 МГц), ГЛОНАСС (L1 – 1602 МГц / L2 – 1246 МГц), BeiDou (B1 – 1561,098 МГц / B2 – 1207,14 МГц / B3 – 1268,52 МГц), Galileo (E1 – 1575,42 МГц / E6 – 1278,75 МГц / E5 – 1191,79 МГц);

- дальность подавления приемных трактов:

а) средств связи на НСУ: до 10–25 км;

б) средств связи на БВС: до 30–50 км;

в) канала ГНСС на БВС: до 30–50 км;

- энергопотенциал воздействия:

а) на канал передачи данных «БВС – НСУ»: 300–500 Вт;

б) на канал управления «НСУ – БВС» и телеметрии «БВС – НСУ»: 500–1000 Вт;

в) на канал ГНСС на БВС: 300–1000 Вт;

- тип формируемых помех:

а) для каналов связи и управления: прицельная и скользящая по частоте, заградительная по диапазону частот;

б) для канала навигации по ГНСС: прицельная по частоте и структуре сигнала с целью формирования ложной навигационной информации (по открытым частотам ГНСС); шумовая прицельная по частоте (по открытым или закрытым частотам ГНСС).

Можно выделить отличительные характеристики небоевых систем РЭП, которым посвящен рассматриваемый материал [8]:

- относительно невысокий энергопотенциал, обеспечивающий требования электромагнитной совместимости (ЭМС) со службами радиосвязи на рабочих частотах за пределами зоны подавления;
- использование направленных антенных систем, обеспечивающих подавление радиоканалов БВС в заданных секторах;
- обнаружение несанкционированных БВС с использованием средств видеоконтроля и неизлучающих средств радиоконтроля (пассивная радиолокация);
- использование подавления каналов управления БВС с использованием помех, совпадающих по частоте и структуре с широко распространенными средствами связи с малыми БВС (квадрокоптерами);
- идентификация каналов управления, основанная на автоматическом определении типа протокола из числа широко распространенных, использование известных уязвимостей в этих каналах;
- использование режимов подавления и навязывания ложных режимов для закрытых каналов навигации ГНСС с формированием шумовых помех, прицельных по частоте, и формирование ложных сигналов имитирующими помехами, настроенными на частоты и структуру навигационных сигналов, для открытых каналов ГНСС («спуфинг», подмена сигналов ГНСС).

ИНФОРМАЦИОННЫЙ РЕСУРС РАДИОКАНАЛОВ БВС В УСЛОВИЯХ РЭП

Зададим информационный ресурс (ИР) несанкционированных БВС как энтропию покрытия [9–11] от способности использования имеющихся радиоканалов в условиях радиоэлектронного противоборства.

Для определения ИР необходимо оценить характеристики радиолиний несанкционированного БВС и определить их предельные значения. Далее информационный ресурс по своему значению покажет степень эффективности РЭП. Информационный ресурс $I_{БВС}$ определим как сумму энтропий покрытия по каждому радиоканалу БВС:

$$I_{БВС} = \sum_{i=1}^{m} H_i, \quad (1)$$

где m – количество радиоканалов БВС, по которым ведется подавление

H_i – ‘энтропия покрытия i-го радиоканала БВС

$$H_i = \begin{cases} \ln\left(\frac{I_i}{P_{\max i\,\text{БВС}}}\right), I_i \geq P_{\max i\,\text{БВС}} \\ 0, I_i < P_{\max i\,\text{БВС}} \end{cases}, \quad (2)$$

где I_i – мощность помехи от средства РЭП на входе приемника i-го радиоканала БВС, СУ БВС; $P_{max\ i}$ БВС – максимальное значение мощности полезного сигнала i-го радиоканала на входе приемника БВС, СУ БВС.

Для радиоканалов с ШПС выражение (2) примет вид:

$$H_i = \begin{cases} \ln\left(\frac{I_{Fi}}{E_{\max i\,\text{БВС}}}\right), I_i \geq P_{\max i\,\text{БВС}} \\ 0, I_i < P_{\max i\,\text{БВС}} \end{cases}, \quad (3)$$

где I_{Fi} – плотность мощности помехи от средства РЭП в полосе частот сигнала БВС на входе приемника i-го радиоканала БВС, СУ БВС; $E_{max\ i\ БВС}$ – максимальное значение энергии полезного сигнала i-го радиоканала на входе приемника БВС, СУ БВС.

Уровень энергии помехи от РЭП должен обеспечить вероятность ошибочного приема символов цифровых систем BER = 0,1 … 0,5 [12]. Расчеты энергетики радиоканалов нежелательно вести для модели распространения радиоволн в свободном пространстве, потому что следует учитывать влияние земной поверхности при прохождении радиоволн в районе наземных средств РЭП и НСУ. Поэтому следует использовать методику, которая приведена в Рекомендации МСЭ-R P.528–3 [13] и позволяет рассчитать бюджет радиолинии с использованием экспериментальных кривых распространения радиоволн для воздушной подвижной и радионавигационной служб, работающих в диапазонах ОВЧ, УВЧ и СВЧ. Для расчетов по данной методике была разработана программа на языке программирования VBA.

Рассмотрим три сценария работы, определяемых типами средств БВС и РЭП:

1) БВС типа Mini – РЭП типа «Репеллент» и мобильная система РЭП с меньшей мощностью передатчика;
2) БВС типа Micro – портативная система РЭП;
3) каналы ГНСС БВС типа Mini – мобильная система РЭП.

Этих сценариев достаточно для выявления особенностей применения существующих средств РЭП в целях противодействия БВС.

Характеристики БВС и средств РЭП, необходимые для проведения расчетов информационной эффективности по указанным сценариям, представлены табл. 5.

В первую очередь необходимо рассчитать потери энергии сигнала в радиоканалах. При расчетах радиолиний в направлениях от наземных радиоэлектронных средств (РЭС) на БИС и от БВС на наземные РЭС, как указывалось выше, была использована модель радиоканала, описанная в [13]. Для ориентировочных расчетов иногда используют модель распространения радиоволн в свободном пространстве [14], но при этом не учитываются ни зоны Френеля, ни затухания в атмосфере и прочие потери. И следует отметить, что разница в расчетах по этим моделям для рассматриваемых радиоканалов может достигать 15 дБ, что недопустимо.

Для расчетов энергетики радиоканалов между наземными РЭС использована модель радиоканала, представленная в Рекомендации МСЭ-R P.1546–5 [15]. Но может быть использована и Рекомендация МСЭ-R P.452 [16]. Однако для расчетов прохождения сигналов по Рекомендации МСЭ-R P.452 требуется знание профиля высот трассы распространения радиоволн.

Следует отметить, что расчеты проведены для оптимальных систем приема сигналов для предельных энергетических ситуаций и могут рассматриваться в качестве потенциально до-

Таблица 5

ХАРАКТЕРИСТИКИ БВС И СРЕДСТВ РЭП, НЕОБХОДИМЫЕ ДЛЯ ПРОВЕДЕНИЯ РАСЧЕТОВ ИНФОРМАЦИОННОЙ ЭФФЕКТИВНОСТИ

ХАРАКТЕРИСТИКИ	ТИП БВС				
	MINI		MICRO		MINI/КАНАЛ GPS
Fc, МГц	145	380	2400	5500	1575,42
БВС э.и.и.м.*, дБВт	14	11,8	10	5	–
НСУ э.и.и.м., дБВт	14	14	-10	-10	–
Расстояние D1 НСУ-БВС, км	0,5; 1,0; 10	0,5; 1,0; 10	0,3; 1,0	0,3; 1,0	–
h1 НСУ, м	10	10	1,5	1,5	–
Высота БВС, м	300	150	70	70	150
РЭП э.и.и.м., дБВт	27,0	7,0	7,0	7,0	7,0
$h_{РЭП}$, м	10	10	1,5	1,5	10
$D_{РЭП-БВС}$, км	0,1	0,1	0,1	0,1	0,1

*Эквивалентная изотропно излучаемая мощность – (э.и.и.м.).

стижимых результатов. Ознакомиться с расчетами и математическими моделями можно в [17].

ЗАКЛЮЧЕНИЕ

В результате проведенного анализа можно сделать вывод о том, что наибольший информационный ресурс имеют средства РЭП типа системы «Репеллент», устанавливаемой на колесном шасси и имеющий наибольшие энергетические характеристики. И по частотным диапазонам, и по типам подавляемых радиоканалов она превосходит другие средства РЭП. Информационный ресурс системы «Репеллент» в зависимости от тактической обстановки меняется от 20 до 45 децидит.

Мобильные средства РЭП имеют достаточный информационный ресурс от 1,5 до 20 децидит только по действию на БВС.

Портативные средства РЭП имеют меньший информационный ресурс и способны обеспечивать достаточный уровень помех на БВС для вероятности двоичной ошибки в районе 0,1.

Все рассмотренные средства РЭП показали хорошее подавление навигационных каналов. Даже для высокой вероятности ошибки, равной 0,45, информационный ресурс очень высокий и составляет не менее 80 децидит для большинства систем РЭП.

Необходимо также отметить, что расчеты энергетики радиоканалов, связанных с БВС, недопустимо вести по широко распространенной модели распространения радиоволн в свободном пространстве. Проведенные сравнительные расчеты показали превышения таких оценок энергетики радиолиний от расчетов по модели радиоканала, приведенной в Рекомендации МСЭ-R P.528, на 15 дБ и более.

Список использованных источников и литературы

1. Ломакин М.И., Докукин А.В., Сланчак О.Ю. [и др.] Оценка и оптимизация качества мониторинга территориально-распределенных объектов, проводимого с помощью беспилотных летательных аппаратов // Информационно-экономические аспекты стандартизации и технического регулирования. 2022. № 3(67). С. 39–42.
2. Бурый А.С., Шевкунов М.А. Оценка качества беспилотных авиационных систем мониторинга окружающей среды // Информационно-экономические аспекты стандартизации и технического регулирования. 2017. № 6 (40). С. 4.
3. Бурый А.С., Шевкунов М.А. Интеллектуальные системы поддержки принятия решений при управлении динамическими объектами // Информационно-экономические аспекты стандартизации и технического регулирования. 2015. № 5 (27). С. 2.
4. Сухов А.В., Величко П.С. Конюшев В.В., Левин А.И. Информационный ресурс в общих технических требованиях к информационно-коммуникационной технологии «цифровая полиция» // Информационно-экономические аспекты стандартизации и технического регулирования. 2022. № 3 (67). С. 56–68.
5. Открытый обзор продукции российских производителей специальных средств и техники для обеспечения общественной безопасности: Научно-технический информационный сборник. Вып. 2 (9). – М.: ФКУ НПО «СТиС» МВД России, 2021. – 68 с.
6. Жданов Ю., Овчинский В. Полиция будущего. [Электронный ресурс]. – М.: 2018. 166 с. – URL: http://ipa-russia.org/библиотека-ассоциации/ (дата обращения: 04.10.2022).
7. Сигналы глобальных навигационных систем [Электронный ресурс]. – URL: https://habr.com/ru/post/680304/ (дата обращения: 04.10.2022).
8. Макаренко С.И. Противодействие беспилотным летательным аппаратам: Монография. – СПб.: Наукоемкие технологии, 2020. – 204 с.
9. Решетников В.Н., Савилкин С.Б., Сухов А.В. Мониторинг частотного ресурса геостационарных спутников-ретрансляторов с использованием энтропии покрытия // Программные продукты и системы. 2017. № 1. С. 119–123.
10. Сухов А.В. Оценка информационного ресурса радионавигационных станций в условиях помех от средств мобильной связи // Правовая информатика. 2019. № 1. С. 36–45.
11. Sukhov A.V. Dynamics of information flows in a control system of a complex technological system // Journalof Computer and Systems Sciences International. 2000. Vol. 39. No 4. P. 592–600.
12. Эффективность системы военной связи: учеб.-метод. пособие / И.О. Мачихо [и др.]. – Минск: БГУИР, 2017. – 102 с.
13. Рекомендация МСЭ-R P.528–3. Кривые распространения радиоволн для воздушной подвижной и радионавигационной служб, работающих в диапазонах ОВЧ, УВЧ и СВЧ. ITU. Женева. 2013.
14. Рекомендация МСЭ-R P.525–3 Расчет ослабления в свободном пространстве. ITU. Женева. 2016.
15. Рекомендация МСЭ-R P.1546–5. Метод прогнозирования для трасс связи «пункта с зоной» для наземных служб в диапазоне частот от 30 МГц до 3000 МГц. ITU. Женева. 2013.
16. Рекомендация МСЭ-R P.452–16. Процедура прогнозирования для оценки помех между станциями, находящимися на поверхности Земли, на частотах выше приблизительно 0,1 ГГц. ITU. Женева. 2015.
17. Сухов А.В., Пузийчук С.И. Информационный анализ эффективности радиопротиводействия беспилотным воздушным судам // Информационно-экономические аспекты стандартизации и технического регулирования. 2022. № 5 (69). С. 58–70.

ОЛЕГ ПЕЛИПАС,
начальник отдела информационной безопасности Российского института стандартизации,
руководитель межведомственной рабочей группы комитета ТПП РФ по безопасности предпринимательской деятельности «Технические средства защиты» (МРГ «Техзащита»),
председатель технического комитета по стандартизации «Средства надежного хранения и безопасности» (ТК 228)

ТРЕБОВАНИЯ К СПЕЦИАЛЬНЫМ ТЕХНИЧЕСКИМ СРЕДСТВАМ ПРОТИВОДЕЙСТВИЯ БЕСПИЛОТНЫМ УСТРОЙСТВАМ: АЛГОРИТМ РАЗРАБОТКИ И ИСПОЛНЕНИЯ

Актуальность разработки нормативной базы для специальных технических средств противодействия (СТСП) беспилотным устройствам продиктована многими факторами. Один из них – стремительное развитие сегмента беспилотных воздушных судов (БВС), спрос на которые увеличивается с каждым годом. В сложившихся условиях особенно важно уточнить требования к современным СТСП БВС, процедуре проверки их функциональности, в т. ч. на объекте для достижения гарантированного результата применения. В статье рассмотрены актуальные задачи в сфере разработки, производства и эксплуатации специальных технических средств обнаружения и противодействия беспилотным устройствам.

НЕМНОГО ПРЕДЫСТОРИИ

Дистанционно управляемые средства поражения известны с 1930-х гг. Спектр этих изделий достаточно широк. Устройства использовались для доставки боевой части до цели с помощью дистанционного управления вектором тяги носителя по командам оператора или по встроенному в головку самонаведения алгоритму ракеты, бомбы или снаряда. При самонаведении уже в те годы применялся анализ изображения и его передача.

В преддверии Второй мировой войны развитые страны вели работы по созданию дистан-

ционно управляемого боеприпаса. Например, в фашистской Германии в секретной лаборатории BMW в конце 1930-х гг. разрабатывалась управляемая противотанковая ракета ПТУР X-7 («Роткэпхен» – «Красная шапочка»).

В 1943 г. немецкие войска впервые применили против цели на море высокоточное оружие с дистанционным управлением, атаковав итальянский линкор Rome. Тогда боеприпас управлялся оператором по радиоканалу.

В 1945 г. США разработали боеприпас с инфракрасным наведением.

В Советском Союзе специалисты занимались высокоточным оружием, начиная с 1930-х гг. Разрабатывались самонаводящиеся («корректируемые») управляемые авиабомбы для применения по морским целям с использованием наведения по изображению; с управлением по радиоканалу на основании изображения с курсовой камеры; с наведением по тепловому излучению и т. п.

Сравнение решений тех лет и современных систем показывает, что принципиально они не отличаются: то же радиоуправление или встроенная программа, те же головки самонаведения по тепловому излучению и т. п. Чертежи первых разработок так же легко перепутать с чертежами современных решений. Ничего удивительного – законы физики для нашей планеты неизменны. Но, как обычно, все решают детали.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Согласно Воздушному кодексу Российской Федерации от 19.03.1997 № 60-ФЗ «…беспилотным называется воздушное судно, управляемое, контролируемое в полете пилотом, находящимся вне борта такого воздушного судна (внешний пилот)». И хотя в Воздушном кодексе речь идет о гражданских воздушных судах, но в целом определения подходят и для управляемого боеприпаса который так же можно отнести к категории беспилотного воздушного судна (БВС), ориентируясь на характеристики полета и управления, а систему его запуска и управления назвать беспилотной авиационной системой (БАС).

Под беспилотной авиационной системой понимается комплекс взаимосвязанных элементов, включающий в себя одно или несколько беспилотных воздушных судов, средства управления полетом одного или нескольких беспилотных воздушных судов и контроля за полетом одного или нескольких беспилотных воздушных судов (станцию внешнего пилота и линию управления беспилотными авиационными системами и контроля беспилотной авиационной системы), а также средства осуществления взлета и посадки беспилотных воздушных судов.

Как показывает практика применения гражданских БВС в зоне проведения специальной военной операции, в «горячих точках» по всему миру или в условиях мирного времени с целью совершения противоправных действий, направленных на подрыв законности и правопорядка, грань, разделяющая боеприпас и гражданское БВС, становится все более тонкой и малозаметной.

Важно отметить, что в Указе Президента Российской Федерации от 17 декабря 2011 г. № 1661 «Об утверждении Списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль» (в ред. от 21.07.2014, 07.04.2017) были упомянуты «Беспилотные (воздушные) летательные аппараты (БЛА) и специально разработанные компоненты (блоки) и комплектующие, а также программное обеспечение для них».

В п. 1 ст. 1 Закона Российской Федерации от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» говорится, что закон регулирует отношения, возникающие при:

– разработке, принятии, применении и исполнении обязательных требований к продукции, в том числе зданиям и сооружениям (далее – про-

дукция), или к продукции и связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации;

– применении и исполнении на добровольной основе требований к продукции, процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, а также к выполнению работ или оказанию услуг в целях добровольного подтверждения соответствия;

– оценке соответствия.

На основании этого можно сделать вывод, что вопрос об оценке соответствия БВС и БАС находится в области стандартизации и технического регулирования.

Это тем более важно, что Федеральный закон от 2 декабря 2019 г. № 404-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» и другие правовые документы наделили правом применения специальных технических средств противодействия беспилотным воздушным судам (СТСП БВС) различные невоенные службы и организации, вплоть до частных охранных организаций.

НА СТЫКЕ ТЕХНОЛОГИЙ И ТРЕБОВАНИЙ ЗАКАЗЧИКОВ

Требования к СТСП определяются самим временем, в частности, тем, что в мире насчитывается около 500 производителей беспилотных воздушных судов. У каждого в линейке моделей – от нескольких штук до нескольких десятков. И все эти поставщики продолжают совершенствовать технологии с учетом современного развития науки, техники и требований заказчика.

Если раньше постановка маскирующих помех служила средством, одинаково хорошо действующим на любое БВС, то сейчас никого не удивить сложными алгоритмами вычитания помехового сигнала, реализуемыми на борту БВС. Работа передатчиков БВС с шумоподобными сигналами, в режиме псевдослучайного переключения несущей частоты, со скоростью, например, 10 Гц, и т. п. являются общими нормами для большей части моделей БВС, что, в свою очередь, предъявляет дополнительные требования к СТСП.

Прежде многие разработчики СТСП БВС использовали в своих изделиях инженерные радиосканеры, простые антенны, излучатели «белого» шума, дешевые погодозависимые локационные станции и многое другое, позаимствованное из основ радиомоделирования. В настоящее время подобные решения не могут служить основой для разработки систем защиты объектов, данных, персонала и т. п. от внешнего воздействия с использованием БВС.

В период стремительного развития технологии на смену энтузиастам-любителям приходят специализированные коллективы профессионалов с уникальным оборудованием и подходами.

Статус СТСП БВС в настоящее время проходит процедуру утверждения. При этом очевидно, что они не относятся ни к техническим средствам охраны, определенным, например, Постановлением Правительства Российской Федерации от 23 июня 2011 г. № 498 «О некоторых вопросах осуществления частной детективной (сыскной) и частной охранной деятельности» или Постановлением Правительства Российской Федерации от 26 сентября 2016 г. № 969 «Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности (в ред. от 17.042021)» и др., ни к техническим средствам охранной сигнализации, ни к инженерно-техническим средствам физической защиты и т. п.

Несмотря на то, что в Постановлении Правительства РФ от 30.12.1999 № 1436 (ред. от 08.12.2023) «О специальных средствах и огнестрельном оружии, используемых ведомствен-

ной охраной» и в Постановлении Правительства РФ от 26.01.2000 № 73 (ред. от 08.12.2023) «Об утверждении Правил приобретения, хранения, учета, ремонта и уничтожения специальных средств, используемых работниками ведомственной охраны федеральных государственных органов, федеральных органов исполнительной власти, высшего исполнительного органа субъекта Российской Федерации – города федерального значения Москвы» «специальные технические средства противодействия беспилотным воздушным, подводным и надводным судам и аппаратам, беспилотным транспортным средствам и иным автоматизированным беспилотным комплексам» указаны в составе специальных средств и индивидуальных средств защиты, но относятся эти постановления только к ведомственной охране.

В свою очередь ведомственная охрана определяется как «совокупность создаваемых имеющими право на создание ведомственной охраны федеральными государственными органами, федеральными органами исполнительной власти, высшим исполнительным органом субъекта Российской Федерации – города федерального значения Москвы и организациями органов управления, сил и средств, предназначенных для охраны объектов в целях предотвращения противоправных посягательств и выполнения иных задач, возложенных на ведомственную охрану», согласно ст. 1 Федерального закона от 14.04.1999 № 77-ФЗ (ред. от 22.04.2024) «О ведомственной охране».

СБАЛАНСИРОВАННАЯ СИСТЕМА МЕР

В сложившейся ситуации особенно важны превентивные меры по регламентированию разработки требований к СТСП БВС, определению процедуры технического соответствия предъявляемым требованиям, проверке их функциональности на конкретном объекте для обеспечения гарантированного результата применения.

Сфера технического регулирования и стандартизации как нельзя лучше подходит в качестве основы подобной системы мер, в том числе в силу глубокой проработки правил и методов подтверждения соответствия.

Работа по созданию системы подтверждения соответствия заявленным требованиям ведется в рамках национальной программы стандартизации на 2024 г. техническим комитетом по стандартизации «Средства надежного хранения и безопасности» (ТК 228) совместно с Российским институтом стандартизации и ведущими производителями СТСП.

В частности, формируется комплекс стандартов «Специальные технические средства обнаружения и противодействия беспилотных устройств», рассматривающих как объект стандартизации специальные технические средства обнаружения и противодействия не только воздушных беспилотных судов, но и водных, а также наземных.

Работа выполняется в партнерстве с крупнейшими заказчиками и производителями СТСП БВС, федеральными органами исполнительной власти, в том числе Минцифры.

В основу разрабатываемых методик заложена задача обеспечения безопасности, и предъявляемые требования рассматриваются именно с этой точки зрения, одновременно учитываются внешние факторы и зависимые объекты.

Параллельно ведется большая методическая работа с целью разъяснения подходов, апробирования методик и уточнения требований с конечным потребителем СТСП БВС.

30 мая 2024 г. в Парке «Патриот» в рамках программы XV Международного салона «Комплексная безопасность» состоялся круглый стол «Специальные технические системы противодействия беспилотным устройствам. Вопросы выбора и обоснования соответствия». Мероприятие, организованное органом по сертификации, компанией-разработчиком СТСП БВС, комитетом ТПП РФ по безопасности предпри-

нимательской деятельности, модерировал эксперт Российского института стандартизации Олег Пелипас.

В работе круглого стола приняли участие представители войск национальной гвардии, госкорпораций, предприятий и системообразующих банков, государственных органов, разработчиков и производителей специальных технических средств обнаружения и противодействия беспилотным судам, общественных организаций, а также Российского института стандартизации.

Генеральный директор Российского института стандартизации Денис Миронов в ходе дискуссии подробно остановился на роли Национальной системы сертификации в области подтверждения соответствия, а также ответил на вопросы аудитории о роли стандартизации в развитии промышленности и сегмента разработки СТСП в частности.

В ходе обмена мнениями эксперты отметили высокое значение работ по подтверждению соответствия СТСП предъявляемым требованиям, в том числе в рамках Национальной системы сертификации.

Важным промежуточным результатом работы Российского института стандартизации в области подтверждения соответствия СТСП БВС предъявляемым заказчиками требованиям служит формирование пилотного проекта по подтверждению соответствия, с участием испытательных лабораторий, органа по сертификации, полигона для полевых испытаний и т. п. в нескольких регионах страны.

Одновременно с подтверждением соответствия предъявляемым требованиям важную роль в нормализации рынка СТСП БВС играет соблюдением разработчиками, производителями и эксплуатантами СТСП БВС положений руководящих документов.

Далеко не каждая упомянутая сторона оборота СТСП БВС знает и исполняет требования Минцифры, сформулированные в документах Государственной комиссии по радиочастотам (ГКРЧ). Соблюдение установленных правил – одно из условий нормализации рынка, поскольку следование требованиям руководящих и нормативных документов, в т. ч. требований эксплуатантов и заказчиков, – это гарантия эксплуатации изделия с заданными характеристиками.

Многие стороны, участвующие в обороте СТСП БВС, не осведомлены о том, что при использовании СТСП БВС они становятся пользователями воздушного пространства Российской Федерации и попадают в сферу регулирования Ространснадзора. На практике это означает, что необходимо учитывать требования к использованию воздушного пространства, которые применимы к БВС.

НИКИТА КУПРИКОВ,
канд. техн. наук, доцент, старший научный сотрудник Института 9 Московского авиационного института (НИУ), главный специалист Российского института стандартизации

К ВОПРОСУ ПРИМЕНЕНИЯ ТЕРМИНОЛОГИЧЕСКИХ СТАНДАРТОВ В ЖИЗНЕННОМ ЦИКЛЕ ИЗДЕЛИЙ ПЕРСПЕКТИВНОЙ АВИАЦИОННОЙ ТЕХНИКИ

Значение стандартизации в жизненном цикле изделий авиационной промышленности невозможно переоценить. Безопасность полетов и качество выпускаемой продукции в большой мере зависят от терминологических стандартов, которые применяются на всех этапах – от проектирования и разработки до производства и эксплуатации. Унификация на производстве и стандартизация – обязательные условия комплексного управления качеством продукции, а также своевременной разработки перспективной авиационной техники. Рассмотрим, какие задачи в этой сфере требуют первоочередного решения и чем может быть полезен российским предприятиям опыт зарубежных стран в области стандартизации продукции военно-промышленного комплекса.

В настоящее время нормативно-правовое регулирование качества продукции, выпускаемой предприятиями оборонно-промышленного комплекса (ОПК), во многом противоречит современным реалиям и не учитывает специфику ОПК как высокотехнологичного экономического сектора.

Цель работы – формирование научно-методического обеспечения (при помощи механизма стандартизации) деятельности по установлению правил и характеристик для их добровольного многократного использования, направленной на достижение упорядоченности в сферах производства и обращения продукции, повышение конкурентоспособности продукции, работ или услуг [1].

Кроме того, требует совершенствования и научно-методического сопровождения управление

качеством продукции ОПК, основу которого составляют такие процессы, как разработка, внедрение и оценка соответствия системы менеджмента качества (СМК) с помощью современных технологий требованиям стандартов ISO 9000.

Следует отметить, что в системе управления качеством продукции ОПК российские предприятия пока не применяют современные информационные технологии, что не позволяет анализировать массивы информации и материалов.

Все это, в свою очередь, не дает возможности обеспечить полноценный управленческий процесс в отношении качества продукции. По уровню внедрения технологий российские оборонные предприятия значительно отстают от аналогичных, но более развитых зарубежных производств, где обеспечивается электронное сопровождение наукоемкой продукции на всех этапах ее жизненного цикла (ЖЦ).

Для конкурентного производства, проектирования и эксплуатации авиационной техники на всех этапах жизненного цикла изделия (ЖЦИ) необходимо применение стандартов [3–17].

В авиационной отрасли стандартизация – обязательное условие проектирования перспективной авиационной техники (рис. 1.).

Стандартизация является одной из основных составляющих комплекса мероприятий, действий и процессов, реализуемых в рамках системы менеджмента качества (СМК). Не следует путать СМК и качество продукции как производное эффективно выстроенной СМК.

Унификация на производстве и стандартизация позволяют комплексно управлять качеством продукции на всех стадиях ее разработки, изготовления и эксплуатации, ускорять разработку техники.

Наличие постоянной практики и опыта использования стандартов – один из базовых навыков инженера, конструктора, любого специалиста в авиационной отрасли независимо от его должности [3–17].

ОСНОВНАЯ ЧАСТЬ

В настоящее время к объектам стандартизации и унификации относятся целые агрегаты (например, узлы связи и катапультные кресла) и системы, процессы и даже отдельные мероприятия (системы менеджмента) в течение ЖЦИ.

Для общего понимания процессов жизненного цикла военной и гражданской авиационной техники стоит внимательно изучить терминологию и основные положения ГОСТ Р 56136–2014 «Управление жизненным циклом продукции военного назначения. Термины и определения», а также ГОСТ Р 56862–2016 «Система управления жизненным циклом. Разработка концепции изделия и технологий. Термины и определения» – базовые документы в этой сфере, доступные для студентов.

В настоящее время наблюдаются рассогласованность действий по обеспечению качества оборонной продукции, дублирование или противоречие осуществляемых в ОПК научно-исследовательских работ и организационных мероприятий по обеспечению качества продукции, в том числе из-за различий понятийного аппарата и номенклатуры изделий[1].

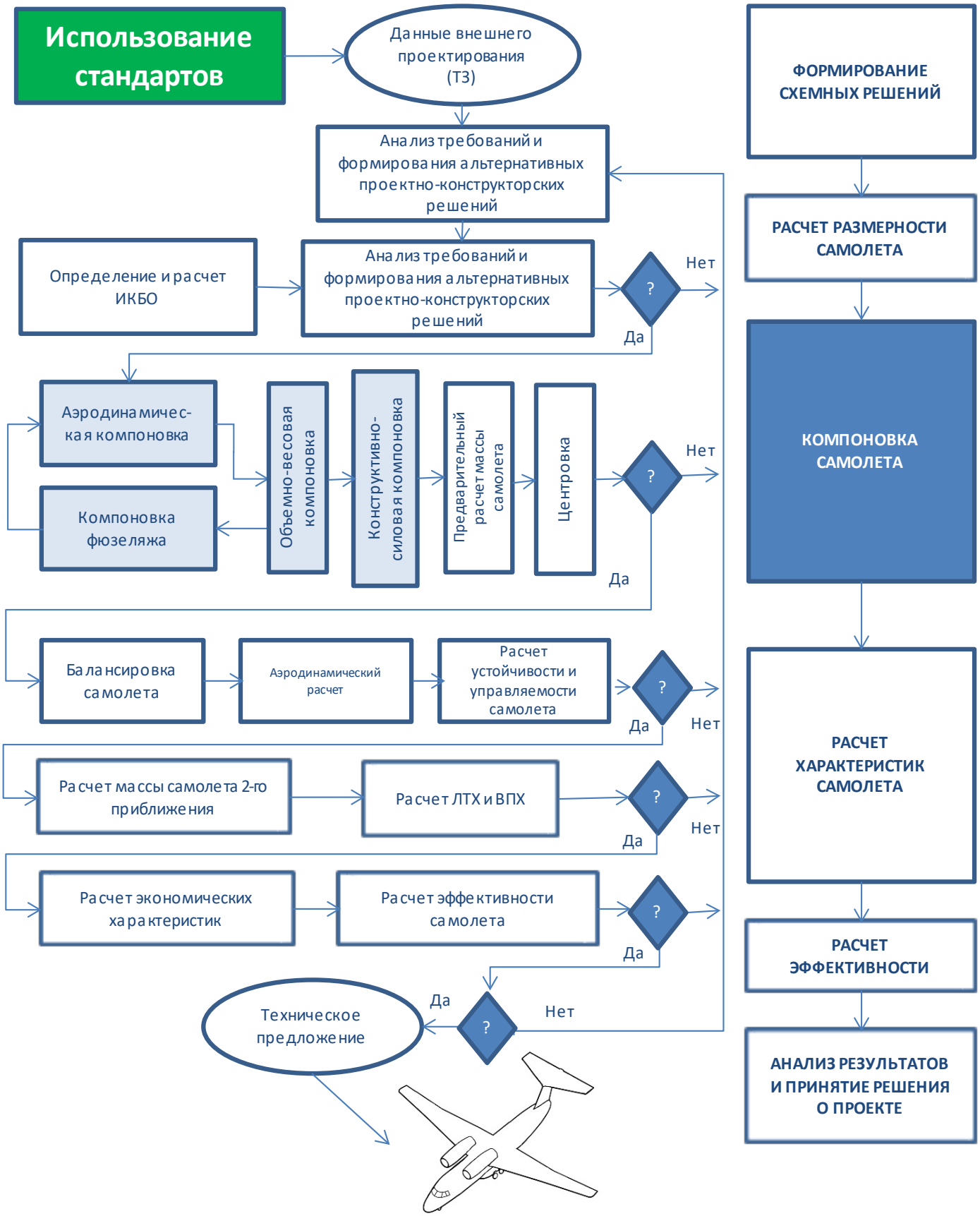
Рассмотрим опыт и практику ведущих зарубежных стран в области стандартизации продукции военно-промышленного комплекса (ВПК).

Так, в США разработка и производство по государственному заказу военной техники регулируются различными документами законодательного и нормативного характера, а также национальными и добровольными стандартами[2].

В НАТО стандартизации продукции ВПК уделяется особое внимание, поскольку, с одной

[1] Сергеев В.Е., Давыдов А.Н., Барабанов В.В. Проблемы обеспечения качества продукции оборонно–промышленного комплекса. – URL: https://cals.ru/sites/default/files/downloads/conf/conf–11–mpnt.pdf

[2] Гончаренко В.И., Мищенко Н.П. Основы стандартизации, унификации и каталогизации оборонной продукции: учебное пособие. – М.: Изд–во ДПК Пресс, 2019. – 296 с. (с. 232).



ДЕКОМПОЗИЦИЯ ПРОЦЕДУР ФОРМИРОВАНИЯ ОБЛИКА САМОЛЕТА

стороны, НАТО обеспечивает эффективность использования экономических ресурсов стран, входящих в этот блок, а с другой – позволяет сохранять целостность альянса и его действенность как военной структуры[3].

В НАТО действуют стандарты двух видов. К первому относятся соглашения STANAG, которые официально закрепляют договоренности нескольких или всех стран – членов НАТО об использовании единых вооружения, военной и специальной техники (ВВСТ) и сопутствующих их применению процессов.

Второй вид стандартов представлен публикациями НАТО – AP, то есть системой документов, используемых несколькими или всеми странами – членами НАТО в целях их применения и распространения до уровня пользователя[4].

Действующая в ЕС достаточно эффективная система стандартизации продукции ВПК способствует повышению конкурентоспособности ВПК ЕС в целом[5]. Основу этой системы составляет Европейское оборонное агентство (EDA), которому подчиняются два комитета по стандартизации: CEN и CENELEC.

Деятельность указанных агентств направлена на то, чтобы стандарты на продукцию ВПК в рамках ЕС были гармонизированы с учетом военных потребностей стран – членов ЕС[6].

Китайская система стандартизации по разработке и созданию ВВСТ находится в стадии реформирования. Основу ее трансформации составляет интеграция гражданских и военных стандартов, а также разработка «пакетов» объединенных стандартов, которые ориентированы на регулирование производства и эксплуатации больших групп ВВСТ[7].

В странах СНГ применяются военные стандарты ГОСТ В и ОСТ В; стандарты, устанавливающие единые требования к продукции ОПК; различные военные дополнения к вышеуказанным документам; стандарты особого периода и дополнения к ним; отраслевые нормативные положения, связанные со стандартизацией ВВСТ.

Все эти документы, признанные межгосударственными стандартами, обеспечивают преемственность нормативно-технической документации каждого государства по отношению к действующей системе стандартов. При этом переоформлять и изменять их не требуется.

Сегодня на современную российскую военную авиационную технику распространяются национальные стандарты ГОСТ РВ и ГОСТ Р, а на авиационную технику, гражданскую авиационную технику могут одновременно распространяться национальные и международные стандарты, нормы Международной организации по гражданской авиации (ICAO), Международной организации по стандартизации (ISO), Международной электротехнической комиссии (IEC), Федерального агентства по техническому регулированию и метрологии (ГОСТ Р), Межгосударственного совета по стандартизации, метрологии и сертификации СНГ (ГОСТ), Американской ассоциации автомобильных инженеров (Society of Automotive Engineers, SAE), а также отраслевые стандарты (ОСТ) и стандарты организации (СТО) и др.

Стандарты международных сообществ и организаций зачастую формируют слишком широкий набор требований, но являются обязательными для авиапроизводителей и перевозчиков, в то время как национальные стандарты, исполь-

[3] Изюмов Д.Б., Кондратюк Е.Л. Научно–технические проблемы стандартизации оборонной продукции за рубежом // Инноватика и экспертиза. – 2019. № 2 (27). – С. 62–72 (с. 70).

[4] Гончаренко В.И., Мищенко Н.П. Основы стандартизации, унификации и каталогизации оборонной продукции: учебное пособие. – М.: Изд–во ДПК Пресс, 2019. – 296 с. (с. 233–234).

[5] Изюмов Д.Б., Кондратюк Е.Л. Научно–технические проблемы стандартизации оборонной продукции за рубежом // Инноватика и экспертиза. 2019. № 2 (27). – С. 62–72 (с. 70).

[6] Гончаренко В.И. … с. 236.

[7] Изюмов Д.Б. … с. 70.

зующие конкретные технические характеристики, не признаются на международном уровне.

Отказ российских авиапроизводителей от применения национальных стандартов совместно со стандартами международных сообществ и организаций на всех этапах жизненного цикла в пользу только стандартов международных сообществ и организаций приводит к гонке за «мнимой» конкурентоспособностью при существенном несоответствии требованиям, отраженным в национальных стандартах (ГОСТ Р).

На территории РФ в рамках системы стандартизации продукции ОПК применяются межгосударственные стандарты с едиными требованиями для оборонной и народно-хозяйственной продукции, а также межгосударственные стандарты с военными дополнениями или дополнениями на период военного положения. Сведения о последних являются составной частью сводного перечня документов по стандартизации[8].

Следует отметить, что в Российской Федерации действуют государственные военные стандарты (ГОСТ РВ) для ВВСТ, которые здесь не рассматриваются.

С 1 сентября 2025 г. не допускается применение отраслевых стандартов, предусмотренных пунктом 6 (подпунктами в, е, и, к, н, о, р, с) Положения о стандартизации в отношении оборонной продукции (товаров, работ, услуг) по государственному оборонному заказу, а также процессов и иных объектов стандартизации, связанных с такой продукцией, которые не включены в сводный перечень документов по стандартизации оборонной продукции или в изменения сводного перечня документов по стандартизации оборонной продукции. Документ утвержден постановлением Правительства РФ от 30 декабря 2016 г. № 1567 «О порядке стандартизации в отношении оборонной продукции (товаров, работ, услуг) по государственному оборонному заказу, продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции, сведения о которой составляют государственную тайну, а также процессов и иных объектов стандартизации, связанных с такой продукцией». *Иными словами, отменяются:*

в) отраслевые военные стандарты;

е) отраслевые стандарты с военными дополнениями к ним;

и) отраслевые военные стандарты с дополнениями к ним на период военного положения;

к) отраслевые стандарты с дополнениями к ним на период военного положения;

н) отраслевые военные стандарты военного положения;

о) отраслевые стандарты военного положения;

р) отраслевые стандарты с едиными требованиями для оборонной и народно-хозяйственной продукции;

с) межгосударственные стандарты, национальные стандарты, отраслевые стандарты и информационно-технические справочники.

Для сохранения используемых отраслевых стандартов в авиационной отрасли предлагается переводить их в форматы корпоративных стандартов или СТО, ГОСТ Р до 2025 г.

При рассмотрении процесса стандартизации в разрезе управления и контроля ее результатов в ходе жизненного цикла можно выделить несколько ключевых элементов:

1) номенклатуру характеристик и показателей, которая включает как действующие показатели (надежность и т. д.), так и новые (стоимость ЖЦ, эксплуатационно-экономическая эффективность и т. д.);

2) систему методов нормирования и расчета показателей;

3) исходные данные, требуемые в расчетах показателей, их состав и возможные способы получения;

[8] Гончаренко В.И. … с. 242–243.

4) процедуры, связанные с разработкой, утверждением и корректировкой комплексных программ по обеспечению избранных параметров в ходе стадий ЖЦ. Данные процедуры могут согласовываться также с иной деятельностью, реализуемой в отношении продукции военного назначения и ее составных частей[9].

Текущие тенденции свидетельствуют о том, что неформально система стандартизации продукции ОПК в РФ не отличается эффективностью, напротив, у нее немало недостатков, что указывает на необходимость ее реформирования[10].

По мнению А. Овчинникова и А. Топчевского, совершенствование системы стандартизации продукции ОПК в РФ в целях повышения ее качества должно сводиться к реализации ряда проектов по разработке государственных военных стандартов в части опытно-конструкторской и технологической деятельности[11].

Кроме того, необходимо активизировать работу по привлечению наработок ОПК гражданского характера в целях совершенствования оборонно-промышленного комплекса с учетом современных требований и инноваций, в которых испытывают потребность вооруженные силы.

В данном случае речь идет о технологиях двойного назначения, способных содействовать развитию промышленного потенциала России[12].

Применение таких технологий и производство на их основе продукции двойного назначения играют значительную роль в сохранении мощности ВПК и ускорении экономического развития государства. При этом за счет получаемой в результате применения двойных технологий прибыли можно компенсировать часть расходов, связанных с разработкой военной техники[13]. ОПК применительно к Российской Федерации служит основным источником высоких технологий, которые применяются в гражданских целях.

Кроме того, создается инновационный фундамент, необходимый для становления гражданской промышленности как высокотехнологичной и конкурентоспособной отрасли. Тем самым сырьевая зависимость России и ее восприимчивость к турбулентности в геополитическом и геоэкономическом пространстве может быть нивелирована[14].

Основу национальной системы стандартизации Российской Федерации составляют технические комитеты по стандартизации (ТК), которые формируют планы по управлению процессами стандартизации, разрабатывают стандарты, проводят их экспертизу. Статус технического комитета установлен статьей 11 закона «О стандартизации в Российской Федерации»[15], а регламенты их создания и функционирования предусмотрены ГОСТ Р 1.1–2013[16].

Технический комитет по стандартизации, который отвечает за работы «по национальной и

---

[9] Судов Е.В., Петров А.Н., Карташев А.В. О концепции стандартизации в области управления жизненным циклом продукции военного назначения // CAD/CAM/CAE Observer. – 2017. – № 4 (112). – С. 39–46. (с. 40).

[10] Там же, с. 43.

[11] Овчинников А., Топчевский А. Стандартизация – основной инструмент обеспечения качества вооружений // Стандарты и качество. – 2016. – № 5 (947). – С. 34–37.

[12] Чистяков М.С. Военно-промышленный комплекс в формировании технологий двойного назначения в развитии гражданской промышленности // Межвузовский сборник статей по материалам IV Всероссийской научно–практической конференции «Социально–экономические и технические проблемы оборонно-промышленного комплекса: история, реальность, инновации». – Нижегородский государственный технический университет им. Р.Е. Алексеева, 2017. С. 105–108.

[13] Бровко П.М., Петрук Г.В. Стратегическое управление развитием предприятий оборонно-промышленного комплекса с использованием двойных технологий ресурсного подхода // Экономические и социальные перемены: факты, тенденции, прогноз. 2016. № 3 (45). С. 82–97.

[14] Чистяков М.С.… с. 108.

[15] Федеральный закон от 29.06.2015 № 162–ФЗ (ред. от 03.07.2016) «О стандартизации в Российской Федерации» // СПС КонсультантПлюс.

[16] ГОСТ Р 1.1–2013 Стандартизация в Российской Федерации. Технические комитеты по стандартизации. Правила создания и деятельности. ФГУП «Стандартинформ», 2014, 23 с.

межгосударственной стандартизации в области интегрированной логистической поддержки и управления жизненным циклом экспортируемой продукции военного и продукции двойного назначения» (ТК 482), утвержден приказом Федерального агентства по техническому регулированию и метрологии от 14 марта 2017 г. № 530, что отражено в соответствующем Положении[17].

В состав ТК 482 входят ведущие компании военно-промышленного комплекса России, такие как ПАО «Компания «Сухой», АО «Корпорация «Аэрокосмическое оборудование», ПАО «Корпорация «Иркут» и др. – в общей сложности более 50 организаций.

ТК 482 разработана «Концепция стандартизации в области управления жизненным циклом продукции военного назначения»[18].

Основные положения данной Концепции заключаются в следующем:

1. Обеспечение единства комплекса общетехнических стандартов и стандартов продукции военного назначения. Такой подход соответствует общей идеологии системы стандартизации в России, согласно которой военные стандарты и стандарты военного положения рассматриваются как приложения к гражданским стандартам. Система стандартизации обеспечивает учет специфики военной продукции; устанавливает режим «двустороннего движения», в рамках которого происходит взаимообогащение гражданских и военных систем стандартизации; повышает рыночную конкурентоспособность товаров и технологий двойного назначения, сокращая издержки, связанные с двойной сертификацией.

2. В качестве базовой позиционируется технология информационной поддержки жизненного цикла изделия. CALS-технологии (Continuous Acquisition and Lifecycle Support) зародились в военно-промышленном комплексе США и неоднократно доказали свою эффективность, обеспечивая снижение стоимости и повышение темпов технологического трансфера. Русскоязычный аналог понятия CALS – аббревиатура ИПИ (Информационная Поддержка процессов жизненного цикла Изделий). Концепция развития CALS (ИПИ) технологий в России[19] разработана и продвигается АО НИЦ «Прикладная Логистика», входящим в состав ТК 482.

3. Понятие «технологии двойного назначения» является довольно «подвижным», так как утверждается соответствующим Указом Президента[20]. Сочетание универсальных технологий (ИПИ) и соотнесение с комплексом общетехнических стандартов позволяет в процессе стандартизации и сертификации продукции оперативно переключаться между режимами: «военная», «двойного назначения», «гражданская», что способствует реализации потенциала ОПК для обеспечения конкурентоспособности отечественной промышленности и при этом не создавать угроз национальной безопасности.

Примером деятельности ТК 482 может служить проект стандарта «Планирование технического обслуживания продукции военного и

[17] Положение о техническом комитете по стандартизации «Поддержка жизненного цикла экспортируемой продукции военного и продукции двойного назначения» (ТК 482) // Приложение к приказу Федерального агентства по техническому регулированию и метрологии от 14 марта 2017 г. № 530. URL: http://tk482.ru/sites/default/files/downloads/pologenie_tk_482_2017.pdf

[18] Концепция стандартизации в области управления жизненным циклом продукции военного назначения. Разработана Техническим комитетом (ТК) Росстандарта № 482 «Поддержка жизненного цикла экспортируемой продукции военного и продукции двойного назначения». Одобрена ТК 482 на заседании, проведенном 08 декабря 2016 г. URL: http://tk482.ru/sites/default/files/downloads/docs/concept_for_web.pdf

[19] Концепция развития CALS-технологий в промышленности России / НИЦ CALS-технологий «Прикладная логистика»; Е.В. Судов, А.И. Левин. – М., 2002, 123 с. URL: http://old.cals.ru/policy/material/concept_ipi.pdf

[20] Указ Президента РФ от 17.12.2011 № 1661 (ред. от 13.12.2018) «Об утверждении Списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль» // СПС КонсультантПлюс.

продукции двойного назначения»[21], который устраняет недостатки аналогичного общетехнического стандарта (ГОСТ Р 27.606), такие как рассмотрение процесса RCM (техническое обслуживание, ориентированное на безотказность) как изолированного; отсутствие учета специфики планирования технического обслуживания в рамках многоуровневых систем технической эксплуатации. В состав стандарта в виде приложений входят «Методические рекомендации по подготовке исходных данных для планирования технического обслуживания» и «Пример представления результатов планирования технического обслуживания».

ЗАКЛЮЧЕНИЕ

Проведенный анализ позволяет сделать вывод, что в России создана система формирования и совершенствования институциональной базы для активизации потенциала отечественного оборонно-промышленного комплекса на основе методов стандартизации и сертификации продукции.

[21] Проект стандарта «Планирование технического обслуживания продукции военного и продукции двойного назначения». URL: http://tk482.ru/sites/default/files/downloads/gost_r_planirovanie_to_produkcii_voennogo_i_produkcii_dvoynogo_naznacheniya_1.0.482–1.015.19.pdf

Список использованных источников и литературы

1. Интернет-сайт Федерального агентства по техническому регулированию и метрологии // Режим доступа: https://www.gost.ru/portal/gost/home/activity/standardization, 01.06.2024.
2. Интернет-сайт Союза авиапроизводителей России. // Режим доступа: http://www.aviationunion.ru/about.php, 01.06.2024.
3. Авиация. Энциклопедия. – М.: Большая российская энциклопедия, ЦАГИ, 1994. – 785 с.
4. Астахов С.А. Состояние и перспективы развития парашютостроения в Российской Федерации. // Журнал Академии Военных Наук. 2015. №2. С.99–113.
5. Долгов О.С., Куприков Н.М., Кутахов В.П. Организационно-экономические механизмы управления развитием системы эксплуатации региональных самолетов в Арктическом регионе Российской Федерации // Вестник Академии Военных Наук, М.: 2014. № 4. С. 99–113.
6. Егер С.М., Лисейцев Н.К. и др. Проектирование самолетов. М.: Машиностроение, 1983. – 395 с.
7. Егер С.М., Лисейцев Н.К., Самойлович О.С. Основы автоматизированного проектирования самолетов. М.: Изд-во. Машиностроение, 1986. – 675 с.
8. Куприков М.Ю. Применение информационных технологий на этапах жизненного цикла изделия // журнал «Качество и жизнь», М.: 2004. № 4. С. 210–22 с.
9. Куприков М.Ю. Структурно-параметрический синтез геометрического облика самолета при «жестких» ограничениях: Учебное пособие. – М.: Изд-во МАИ, 2003. – 112 с.
10. Компоновка самолетов. Под ред. М.Ю. Куприкова. – М.: Изд-во. МАИ, 2012. – 272 с.
11. Егер С.М., Лисейцев Н.К., Самойлович О.С. Основы автоматизированного проектирования самолетов. М.: Изд-во. Машиностроение, 1986. – 676 с.
12. Карапетян Т.С. Проектирование кабины экипажа пассажирского самолета транспортной категории. – М.: Изд-во МАИ, 2014. – 178 с.
13. Мальчевский В.В. Матрично-топологический метод синтеза схемы и компоновки самолета (опыт автоматизации творческой деятельности конструктора). – М.: Изд-во МАИ, 2011. – 124 с.
14. Рухлинский В.М. Методология формирования обликовых эксплуатационно-технических характеристик высокоэффективных самолетов нового поколения: Диссер. на соиск. уч. степ. докт. техн. наук. Москва, 2015. – 157 с.
15. Технология самолетостроения / Под общ. ред. А.Л. Абибова. – М.: Изд-во. Машиностроение, 1970. – 230 с.
16. Основы авиационной техники: Учеб. для студентов вузов, обучающихся по направлению «Авиа- и ракетостроение» / С.М. Егер, А. М. Матвеенко, И.А. Шаталов. Под ред. И.А. Шаталова. – 2-е изд., перераб. и доп. – М.: Изд-во МАИ, 1999. – 575, [1] с. : ил.
17. Левицкий В.С. Машиностроительное черчение и автоматизация выполнения чертежей. – М.: Высшая школа, 1998 г. – 442 с.