США & Канада: экономика, политика, культура / USA & Canada: economics, politics, culture 2020; 50(10): 5-25

УДК 327; 327.3
DOI: 10.31857/S268667300011803-3

О подходах к обеспечению кибербезопасности систем управления ядерным оружием

П. С. Золотарёв
Институт США и Канады РАН (ИСКРАН)
Российская Федерация, 121069 Москва, Хлебный пер., 2/3
ORCID: 0000-0003-1493-0455 p.zolotarev@iskran.ru
Статья поступила в редакцию 14.07.2020.

Резюме: В статье рассмотрена роль информационных систем в развитии человечества на данном историческом этапе. Сделан вывод о том, что скорость совершенствования информационных систем, создавая условия для высоких темпов всестороннего развития, порождает возникновение широкого спектра угроз, в том числе в области управления ядерным оружием. На основе анализа доктринальных документов России и США по вопросам информации показана суть разных подходов к обеспечению безопасности в этой области. Обосновывается, что обеспечение безопасности систем управления ядерным оружием относится к сфере общих интересов России и США, не зависящей от текущих политических отношений между двумя странами. Даётся анализ ключевых элементов системы управления ядерным оружием (основной и резервной) с точки зрения уязвимости от постороннего вмешательства и создания угроз безопасности. Затронуты проблемные вопросы систем предупреждения о ракетном нападении, космического сегмента систем управления ядерным оружием, процедур принятия решений на применение ядерного оружия и особенностей, связанных с управлением нестратегическим ядерным оружием. В статье содержаться рекомендации по повышению защищённости систем управления ядерным оружием, которые могут быть востребованными для всех ядерных государств, включая Китай.

Ключевые слова: кибербезопасность, ядерная политика, ядерное оружие, СПРН, США, Россия, Китай

Для цитирования: Золотарёв П.С. О подходах к обеспечению кибербезопасности систем управления ядерным оружием. *США & Канада: экономика, политика, культура* 2020; 50 (10) 5-25. DOI: 10.31857/S268667300011803-3

Approaches to Ensuring Cybersecurity of the Nuclear Weapons Control Systems

Pavel S. Zolotarev
Institute for the U.S. and Canadian Studies,
Russian Academy of Sciences.
2/3 Khlebny per., Moscow 121069, Russian Federation
ORCID: 0000-0003-1493-0455 e-mail: p.zolotarev@iskran.ru
Received 14.07.2020.

Abstract: The article considers the role of information systems in the development of mankind at this historical stage. It is concluded that high rates of improvement of information systems, creating conditions for high rates of comprehensive development, give rise to a wide range of threats, including in the field of nuclear weapons management. Based on the analysis of doctrinal documents of Russia and the United States in the information sphere, the essence of different approaches to ensuring security in this sphere is shown. It is proved that ensuring the security of nuclear weapons control systems belongs to the sphere of common interests of Russia and the United States, independent of the current political relations between the two countries. The analysis of the key elements of the nuclear weapons control system (main and backup) from the point of view of vulnerability from outside interference and creating security threats is given. Problematic issues of missile attack warning systems, the space segment of nuclear weapons control systems, decision-making procedures for the use of nuclear weapons, and features related to the management of non-strategic nuclear weapons were discussed. The article contains recommendations for improving the security of nuclear weapons control systems, which may be in demand for all nuclear-weapon states, including China.

Keywords: cybersecurity, nuclear policy, nuclear weapons, early-warning radar, USA, Russia, China

For citation*:* Zolotarev P.S. Approaches to ensuring the cybersecurity of the nuclear weapons control systems. *USA & Canada: Economics, Politics, Culture.* 2020; 50 (10) 5-25. DOI: 10.31857/S268667300011803-3

ВВЕДЕНИЕ

Известно, что формы и способы информационного взаимодействия, наряду со свойством материи к самоорганизации, создают основу для развития. Преимущество человека над другими представителями живого мира состоит в том, что человек научился накапливать, хранить и передавать информацию путями, отличными от тех, которые заложила природа в живые организмы. За многие тысячелетия своей истории человек освоил всего два способа обмена информацией – с помощью речи (звуковые волны) и визуальных изображений (буквы, иероглифы и т. д.). В зависимости от степени овладения и использования этих способов информационного взаимодействия сложился современный уровень развития – от племён на первобытнообщинном уровне до государств с высоким уровнем жизни, науки, экономики, культуры и образования.

Заметные импульсы ускорения темпов развития человечества связаны с освоением технологий обмена информацией. Первым таким импульсом стало освоение технологий книгопечатания. Второй импульс (с середины XIX до второй половины XX века) связан с повышением скорости обмена информацией на большие расстояния (электросвязь и радиосвязь). Третий импульс (с конца XX века по настоящее время) связан с качественным скачком скорости, объёма и пространства распространения информации. Именно качественный скачок в развитии информационных технологий запустил процессы глобализации. Первоначально появилась возможность глобализации в сфере производства, когда

управление транснациональными компаниями перестало зависеть от расстояния между администрацией компаний и производственными подразделениями. Дальнейшее повышение скоростей обмена и объёма информацией создало условия для появления глобальной финансовой системы (глобальный банкинг и т. д.). Человечество приобретает черты единой системы, все элементы которой взаимосвязаны в реальном масштабе времени независимо от географического положения. В то же время возникший импульс многостороннего развития во всех сферах жизнедеятельности закономерно привёл к использованию информационного пространства и во всех сферах противоборства интересов (от межличностного до межгосударственного). Кроме того, вытеснение информационными системами надёжных, оправданных временем, далеко уступающих по своим возможностям старых способов информационного взаимодействия приводит к росту зависимости от современных информационных систем, в значительной степени уязвимых не только от злонамеренного вмешательства человека, но и от природных явлений.

Рост возможностей сопровождается ростом уязвимости. Чем выше в государстве уровень развития информационных сетей, тем больше внимания оно вынуждено уделять вопросам информационной безопасности. Это хорошо видно на примере Соединённых Штатов Америки.

Стратегия сохранения глобального лидерства США выстраивается на том, что необходимо акцентировать усилия не на готовности к происходящим в мире изменениям, а создавать и контролировать само будущее. Реализация этой стратегии связана с обеспечением превосходства США в ряде ключевых технологий, определяющих будущее, к числу которых отнесены информационно-коммуникационные и космические технологии. Глобальные интересы требуют и глобальных информационных возможностей. Поэтому заслуга США в формировании глобальной информационно-коммуникационной сети вполне закономерна, отвечая потребностям и соответствуя возможностям страны. Достаточно чётко и недвусмысленно обозначено отношение к роли информационных систем в Стратегии национальной безопасности Дональда Трампа, принятой в 2017 г.: «Конкуренция в информационной области ускоряет развитие в политической, экономической и военной областях. Данные, как и энергия, будут формировать экономическое процветание США и наше будущее стратегическое положение в мире. Способность использовать силу данных имеет основополагающее значение для дальнейшего роста экономики Америки» [1].

В то же время США первыми ощутили и те угрозы, которые возникают в информационном пространстве. Их особенность – малые затраты на осуществление кибератак и масштабность разрушительных последствий в различных сферах жизнедеятельности. В докладе «Дорога к кибермощи», подготовленном в США в 2009 г., отмечается, что «стремление стать ″кибердержавой″ является целью стра-

тегии в области информационной безопасности, соответственно, достижение могущества в киберпространстве становится одним из ключевых аспектов политики» [Роговский Е.А. 2014: 198]. Как известно, коммуникационные сети глобального охвата главным образом опираются на космические средства. Именно космические системы связи наилучшим образом позволяют сочетать глобальность охвата и гибкость реагирования на ситуации, требующие оперативного сосредоточения возможностей в определённых регионах (театрах военных действий – ТВД).

Поэтому закономерно, что после террористических атак 11 сентября 2001 г. США одновременно сосредоточили внимание на вопросах кибербезопасности и космической безопасности. Так, специально созданная комиссия под руководством Д. Рамсфелда в 2001 г. представила доклад, в котором, оценивая последствия возможной неожиданной атаки на космические системы своей страны, применила термин «космический Пёрл-Харбор». На основе выводов комиссии Рамсфелда США приступили к выработке политики обеспечения безопасности своих объектов в космосе. В 2018 г. была принята действующая Национальная стратегия по космосу, осенью 2019 г. воссоздано Космическое командование США, образован новый род войск (пока в составе ВВС), в перспективе новый вид вооружённых сил – Космические силы США (*USSF*), наконец, в июне 2020 г. принята Стратегия обороны в космосе (*DSS*) [2]. Таким образом к настоящему времени в США создана структура, обеспечивающая как присутствие американских вооружённых сил в космосе, так и командование и управление операциями в космосе в соответствии с принятыми доктринальными документами. Главная цель – обеспечить доминирование и способность предотвращать любые угрозы интересам США в космическом пространстве.

Параллельно в США развернулись работы в сфере безопасности киберпространства. В 2003 г. была принята «Национальная стратегии безопасности киберпространства» (*National Strategy to Secure Cyberspace)* [3], в 2011 г. – «Международная стратегия США в отношении киберпространства. Процветание, безопасность и открытость сетевого мира» (*International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World) [4]* и в 2018 г. – «Национальная киберстратегия Соединённых Штатов Америки» (*National Cyber Strategy of the United States of America*) [5]. В информационном пространстве США ставят перед собой цель сохранить глобальное превосходство. В сфере кибербезопасности они делают акцент на обеспечении условий для полного использования возможностей информационных систем в интересах развития во всех сферах, подчёркивая, что для этого необходимо обеспечивать свободу действий в информационном пространстве. Одновременно ставится задача сдерживать возможные кибератаки, с упоминанием государств, создающих, по их мнению, угрозы в киберпространстве. В их числе значится и РФ. В этих документах не просматривается непосредственная обеспокоенность США возможностью таких атак на системы управления ядерным оружием, хотя очевидно, что при упоминании угроз кибератак на критические элементы инфраструктуры подразумеваются и системы военного управления.

В России первая Доктрина информационной безопасности была принята в 2010 г., однако, учитывая динамику развития информационных систем и угроз в информационной сфере, в 2016 г. была принята новая Доктрина в этой сфере. В российском документе, как и в американских, обозначена обеспокоенность возможными кибератаками на объекты критической инфраструктуры; значительное внимание уделено проблеме отставания России в развитии информационных технологий и научных исследований в этой сфере. Исходя из оценки реальных возможностей России в Доктрине зафиксирована уязвимость от внешних информационных угроз. При этом информационные угрозы рассматриваются в широком диапазоне – от дестабилизации социально-политической обстановки в стране до уязвимости критических объектов её инфраструктуры.

Сравнивая доктринальные документы России и США в информационной сфере, следует отметить, что в них не предусматривается проведение наступательных кибератак. В то же время дестабилизирующим фактором называется значительный дисбаланс возможностей в сфере кибербезопасности и информационной безопасности в целом. У Соединённых Штатов возникают опасения, что Россия из-за отставания может быть склонна к скрытым кибератакам в форме несимметричных действий. РФ, в свою очередь, вправе опасаться открытых действий США, способных нанести существенный ущерб, на которые она не сможет адекватно отреагировать.

Однако представляется, что применительно к системам управления ядерным оружием ни у России, ни у США нет особой обеспокоенности перспективой взаимных кибератак. Каждая сторона понимает, что такая атака может иметь крайне опасные последствия, вплоть до ядерной войны. В доктринальных документах каждой из сторон есть положения, которые в той или иной форме дают основания предполагать возможную реакцию на такие действия. Так, в утверждённых 2 июня 2020 г. «Основах ядерной политики Российской Федерации в области ядерного сдерживания» к условиям, определяющим возможность применения ядерного оружия, отнесено воздействие противника на критически важные государственные или военные объекты, вывод из строя которых может привести к срыву ответных действий ядерных сил [6].

Таким образом, можно сделать вывод, что проблема кибербезопасности систем управления ядерным оружием России и США актуальна, но не столько в плане взаимных угроз, сколько с учётом возможных атак со стороны других государств или негосударственных структур. Следовательно, есть основание утверждать, что у России и США имеется в этой области совпадение интересов и необходимость сотрудничества. Кроме того, в силу объективной логики системы управления ядерным оружием России и США во многом схожи.

2020; 50(10): 5-25 США & Канада: экономика, политика, культура / USA & Canada: economics, politics, culture

ОСНОВНЫЕ ОСОБЕННОСТИ СИСТЕМ УПРАВЛЕНИЯ ЯДЕРНЫМ ОРУЖИЕМ РОССИИ И США

Напомним, что структуры стратегических ядерных сил и России, и США представляют собой триады, включающие в свой состав межконтинентальные баллистические ракеты (МБР) наземного базирования, баллистические ракеты подводных лодок (БРПЛ) и авиацию стратегической дальности, способную доставлять до цели ядерные бомбы либо крылатые ракеты с ядерной головной частью. Каждый из компонентов стратегических ядерных сил имеет свои особенности. Так, БРПЛ обладают высокой живучестью в условиях ядерного воздействия. Фактически они составляют потенциал, гарантирующий возможность проведения ответного удара.

У США основной стратегический ядерный потенциал сосредоточен именно на подводных лодках. У России – на наземных МБР. Для повышения ядерного потенциала, способного к применению в условиях ядерного воздействия, часть наземных МБР создана в варианте подвижных ракетных комплексов.

Такие особенности стратегических носителей ядерного оружия вызывают соответствующие требования к системам управления. Очевидно, что если есть носители, способные сохраниться после ядерного нападения, то должна быть и система управления, способная сохраниться в этих условиях. Поэтому оба государства создали системы управления стратегическим ядерным оружием [Ярынич В. 2002], позволяющие обеспечить надёжное управление не только в мирное, но и в военное время в условиях применения как обычных, так и ядерных средств поражения. Даже после нанесения противником массированного ядерного удара система управления должна обеспечивать проведение ответного удара с привлечением всего сохранившегося ядерного потенциала. Это требование логично связано с сутью стратегической стабильности – поддержанием состояния «взаимного гарантированного уничтожения».

Требования к надёжности системы управления после ядерного воздействия привели к тому, что оба государства пошли по пути создания помимо основных ещё и так называемых резервных систем управления [7]. Они могут включать в свой состав высокозащищённые стационарные или подвижные (воздушные) запасные пункты управления и ретрансляторы [Ярынич В. 2002].

Для Соединённых Штатов резервная система управления должна быть ориентирована на способность довести приказ после ядерного воздействия до подводных лодок, находящихся в подводном положении. Такую возможность могут обеспечить только радиоканалы низкочастотного диапазона. Скорость в этом диапазоне низка, размеры антенн должны быть соизмеримы с длиной волны (в районе 1,5 км), а мощность сигнала должна быть высокой. Очевидно, что создать высокозащищённый наземный объект с равно защищённым антенным полем весьма проблематично. Поэтому США пошли по пути создания резервной системы управления на базе воздушных пунктов управления и системы воз-

душных ретрансляторов с бортовыми низкочастотными радиопередатчиками и выпускными антеннами соответствующей длины.

Для России ситуация несколько иная. В чрезвычайных условиях после ядерного воздействия необходимо обеспечить надёжное доведение приказов и до подводных лодок, и до МБР наземного базирования. Но до МБР приказ может доводиться в высокочастотном диапазоне, то есть с высокой скоростью.

При имеющихся различиях резервных систем управления России и США общим является использование в этих системах радиоканалов связи различного частотного диапазона, обеспечивающих доведение информации в условиях ядерного воздействия. После окончания холодной войны сначала США, а затем и Россия прекратили нахождение основных элементов резервных систем управления в состоянии постоянной боевой готовности в условиях мирного времени, но готовность к развёртыванию при повышении боевой готовности поддерживается. Использование в резервных системах радиоканалов даёт основание предполагать возможность внешнего вмешательства, но маловероятно, что обстановка после ядерных ударов может позволить проводить какие-либо кибератаки на элементы этой системы. В то же время в ходе военного конфликта нельзя исключать воздействие на отдельные элементы резервных систем управления, например, космические аппараты. Но это уже не относится к кибератакам. В целом представляется, что анализ возможных последствий кибератак на резервные системы управления пока не актуален. Но тем не менее полностью исключать резервные системы управления из сферы внимания на киберуязвимость нельзя. Не исключено, что детальный анализ возможных сценариев проявления ядерного сдерживания в региональных конфликтах может выявить факторы, способные привести к таким угрозам.

Смещение проблем безопасности с глобального уровня на региональный, региональный акцент США в политике ядерного сдерживания, новые государства с ядерным оружием, прекращение действия Договора о ракетах средней и меньшей дальности, появление гиперзвуковых и крылатых ракет в ядерном оснащении требуют более внимательного рассмотрения всех возможных последствий, учитывающих в том числе киберугрозы.

РОЛЬ СИСТЕМ ПРЕДУПРЕЖДЕНИЯ О РАКЕТНОМ НАПАДЕНИИ

Концентрируя внимание на киберуязвимости основной системы управления, необходимо отметить, что ключевая функция этой системы – предоставление высшему руководству страны достоверной информации о фактах применения ядерного оружия. При этом система управления должна обеспечить руководство страны достаточным временем для принятия решения и доведения приказов на применение ядерного оружия в кратчайшие сроки.

Решающую роль в предоставлении достоверной и своевременной исходной информации для принятия высшим руководством решения о применении ядерного оружия играет Система предупреждения о ракетном нападении (СПРН). Такая система имеется и у России, и у США. Но одновременно СПРН можно с полным основанием считать одним из наиболее уязвимых элементов всей системы управления ядерным оружием.

После принятия высшим руководством решения о применении ядерного оружия, доведение приказов непосредственно до оружия занимает незначительное время, даже учитывая необходимость выполнения операторами боевых расчётов действий по вводу пусковых приказов. Поэтому основной резерв увеличения времени, а значит и снижения риска принятия ошибочного решения, связан с совершенствованием СПРН, включая и алгоритмы её работы.

В 1992 г. предпринимались попытки ведения совместных российско-американских работ в рамках проекта РАМОС (*RAMOS – Russian-American Observation Satellite Program*), который был открыт по инициативе президентов США и России (У. Клинтона и Б. Ельцина) [8]. Авторы проекта предусмотрели совместную разработку в рамках проекта двух спутников, по одному с каждой стороны. Предполагалось использование принципа стереоскопической съёмки одного и того же места этой парой спутников с последующим формированием банка данных, который обе страны могли бы в дальнейшем использовать для своевременного обнаружения любой запущенной баллистической ракеты по её характерным признакам.

На начальном этапе реализации программы в 1995–1999 гг. обе страны достигли определённого научно-технического прогресса: были проведены эксперименты в приземной атмосфере и космосе с использованием самолётов-лабораторий и космических аппаратов из состава орбитальных группировок России и США. Однако после решения США выйти из Договора по ПРО и намерения создать национальную систему противоракетной обороны в Вашингтоне стали проявлять беспокойство по поводу безопасности накопленной по программе информации и возможности утечки применяемых в РАМОС американских космических технологий из области противоракетной обороны. Затем возникли сложности с финансированием проекта. В итоге в 2004 г. выполнение программы прекратилось [9], но обстановка в космосе за прошедшее время существенно изменилась, и проблема надёжного функционирования космических аппаратов СПРН приобрела большую актуальность.

Проблемы в космосе связаны с несколькими тенденциями. Например, наметилась тенденция значительного увеличения количества космических аппаратов различного назначения, принадлежащих, в том числе, негосударственным структурам. В результате увеличивается риск случайного или преднамеренного воздействия на космический эшелон СРПН различными методами – от электромагнитных до кинетических. Рост количества космических аппаратов связан, в частности, с планами компании «Спейс-Х» (*Space-X*). По этим планам в интере-

сах развития космического сегмента интернета планируется иметь более 11 000 спутников на различных орбитах с регулярным пополнением группировки по мере ухода оттуда части спутников, в первую очередь с низких орбит. Одновременно одним носителем запускается до 60 микроспутников [10] (13+14), в перспективе – 240. Использование для манёвров космических аппаратов электростатических двигателей выходит за возможности существующих методов расчёта траекторий и традиционных алгоритмов, используемых системами контроля космического пространства как в США, так и в России. В результате увеличивается время прогноза траекторий манёвра и времени предупреждения о возможном столкновении космических аппаратов.

В складывающейся ситуации наибольшую опасность вызывает неопределённость с возможными угрозами космическим аппаратам СПРН России и США, а также космическим аппаратам, задействованным в контуре системы боевого управления ядерным оружием двух ведущих ядерных держав. Но нуждаются в более детальном изучении и возможные последствия ситуаций, когда одновременно выведенное большое количество спутников в течение определённого времени (до разведения каждого на свою орбиту) остаётся в ограниченном пространстве на орбите выведения.

Следует отметить и тенденцию увеличения космического мусора. Повышается риск случайного столкновения и вывода из строя космических аппаратов. При этом истинная причина вывода их из строя будет далеко не очевидной, что может вызывать не только рост взаимной подозрительности, но и приводить к неадекватной реакции.

В условиях существующего недоверия и сложных политических отношений между Россией и США возникают не только опасения неадекватного реагирования на возможные нарушения работы космических аппаратов в системе управления ядерным оружием, но не исключается и начало вывода оружия в космос. Нельзя исключать и преднамеренное физическое уничтожение средствами третьей стороны космических аппаратов из состава первого эшелона СПРН в угрожаемый период с целью провокации конфликта между Россией и США.

Представляется, что при таком развитии космической обстановки целесообразно предусмотреть налаживание между Россией и США такого же продуктивного взаимодействия, как и в сфере предотвращения террористических угроз. С этой целью было бы полезно Министерству обороны РФ организовать совместно с Министерством обороны США прямое взаимодействие соответствующих структур, контролирующих космическое пространство, для своевременного обнаружения и нейтрализации угроз космическим аппаратам, в первую очередь, задействованным в контуре управления ядерным оружием.

Угроза преднамеренного уничтожения относится и к элементам второго эшелона СПРН – радиолокационные станции, имеющие значительные габари-

ты и незащищённые центры обработки информации, что делает их легко уязвимыми при применении обычных средств поражения.

У России и США достаточно здравого смысла, чтобы не допустить удары по объектам СПРН в условиях гипотетического военного конфликта, но со стороны третьей стороны такие провокационные действия исключать нельзя. Более того, нельзя исключать комплексное и целенаправленное воздействие на первый и второй эшелоны ПРО с одновременным внедрением в радары и спутники ложной информации о ядерном нападении.

В связи с этим важное значение имеет единая трактовка и понимание критериев и алгоритмов, по которым будет признан факт того или иного события. Согласованные характеристики технических решений, используемых государствами, создающими или имеющими СПРН, могли бы позволить избежать ошибок в процессе принятия решения. Особенно важно такое снижение вероятности ошибочных решений на применение ядерного оружия в условиях дефицита времени у руководителей ядерных государств.

В практике эксплуатации имеющихся на вооружении ядерных средств уже отмечены случаи ложных тревог, технических сбоев, которые могли бы привести к ложным предупреждениям о нападении, парализовать работу критически важных каналов коммуникаций, прекратить доступ к информации, поставить под удар системы ядерного планирования и средства доставки ядерных сооружений и в конечном счёте привести к развязыванию войны.

После появления у Китая своей СПРН будет уже три государства, способных на основании информации от этих систем проводить ответные действия в форме ответно-встречного удара. Возможно, что это и полезно для эффективности ядерного сдерживания, но при этом неизбежно возрастает риск ошибочных решений.

В складывающихся условиях представляется целесообразным России, США и Китаю провести согласование технических решений, критериев и алгоритмов, применяемых для определения факта пуска ракеты. Оптимальным было бы решение этих вопросов на рабочем уровне взаимодействия министерств обороны. В этом случае ход таких работ можно сделать независимым от оперативно меняющейся ситуации с политическими отношениями государств.

При всей важности принятия технических мер по минимизации риска ошибок в системе СПРН, самым действенным способом его снижения явилась бы реанимация идеи о создании совместного Центра обмена данными от Систем предупреждения о ракетном нападении. Подписанный президентами России и США в 2000 г. Меморандум о создании Центра был рассчитан на 10 лет. На завершающей стадии создания Центра, когда оставались нерешёнными лишь несколько второстепенных технических вопросов, у обеих сторон не хватило политической воли их решить до истечения срока действия Меморандума. Сегодня политический фон значительно сложнее, однако реальная потребность в такой структуре стала значительно выше. Одновременно есть общее желание вовлечь Китай в переговорные процессы по ядерным вооружениям.

К переговорам по сокращению ядерных вооружений нет оснований для привлечения Китая. Но к решению вопросов, связанных со снижением риска принятия ошибочных решений, способных привести к применению ядерного оружия, вполне реально привлечь Китай. Не лишне напомнить, что положения Меморандума предусматривали возможность участия в работе Центра представителей других государств. Сегодня необходимо ставить вопрос об участии в работе Центра представителей всех пяти официально признанных ядерных государств.

Опыт эксплуатации СПРН показывает, что даже в условиях мирного времени представление военно-политическому руководству ошибочной информации о фиксации факта пуска баллистических ракет приближает к начальной фазе процесса принятия решения на ответные действия.

При реализации замысла о создании Центра обмена данными можно было бы пересмотреть существующие алгоритмы действия по сигналам СПРН. Также вполне возможно в мирное время исключить предоставление оперативной информации о поступающих сигналах от СПРН высшему руководству страны. Применение ядерного оружия в мирное время исключено, поэтому такие сигналы могут быть только ложными (внутренние ошибки в СПРН, последствия возмущения электромагнитного поля Земли и т.д.). Совместные расчёты Центра обмена данными позволили бы достаточно быстро определить источник появления ложных сигналов и ограничиться лишь последующим информированием руководства (не обязательно высокого уровня) об имевшем место событии. Однако реализация такого подхода вряд ли может быть осуществимой в случае развёртывания Североатлантическим блоком ракет средней и меньшей дальности в Европе или нахождения сил американского флота на удалениях, позволяющих наносить соответствующими средствами обезглавливающий удар. При таком развитии событий российская сторона с высокой вероятностью может пойти на использование в критической ситуации алгоритмов автоматического формирования приказов на пуск.

ПРОБЛЕМЫ СИСТЕМЫ ПРИНЯТИЯ РЕШЕНИЙ

Несмотря на возможности совершенствования СПРН, её предельные способности по увеличению времени для принятия решения ограничены и зависят от современного уровня развития науки и технологий. Может быть в будущем произойдёт какой-то скачок в их развитии и появится возможность построения СПРН на новых физических и технических принципах, однако сегодняшний лимит времени катастрофически мал и составляет единицы минут [4][5]. Этого времени совершенно недостаточно для принятия сбалансированного решения на применение ядерного оружия с учётом психологического состояния тех, кто принимает решение, необходимости оценки данных СПРН, выбора плана боевого применения и проведения пусковых процедур. В то же время потенциаль-

ная уязвимость СПРН от внешних факторов, возможность сбоев (ошибок) в ключевые моменты заставляют искать резервы этого времени.

В этой связи заслуживает внимания предложение, изложенное в материалах Инициативы по ядерной угрозе (*Nuclear Threat Initiative's*, *NTI)* о принятии президентом решения *под нападением* [11], когда при фиксации старта ракет противника отдаётся приказ не на проведение пуска немедленно, а по истечении определённого времени, например, через несколько часов. Практически это означает сознательную готовность при сомнениях в достоверности информации СПРН пойти на проведение ответного удара. При этом приказ отдаётся немедленно, а значит с высокой вероятностью будет доведён до самого последнего исполнительского уровня. Успех проведения ответного удара фактически будет зависеть только от живучести носителей ядерного оружия.

Учитывая, что основной ядерный потенциал США сосредоточен в морской компоненте стратегических ядерных сил (СЯС), такой вариант соответствует условию «взаимного гарантированного уничтожения» и, соответственно, не нарушает стратегической стабильности. Для России ситуация отличается: её основной потенциал стратегических ядерных сил сосредоточен в наземном компоненте, который, несмотря на наличие подвижных комплексов, отличается меньшей живучестью по сравнению с морским компонентом. Тем не менее, в зависимости от конкретной ситуации, для России тоже может быть приемлемым вариант ответного удара. Так, если между ядерными странами будет договорённость о недопустимости воздействия по объектам стратегических ядерных сил, включая систему управления, а удар противника не носит явно разоружающего характера, то вариант реакции и форма ответного удара могут быть приемлемыми.

Что касается возможностей систем управления России и США, то, несмотря на предпочтение в интересах кибербезопасности аппаратных способов реализации алгоритмов работы, обе системы обладают необходимой гибкостью для осуществления разных вариантов проведения ударов с вариациями и по масштабу, и по пространственно-временной структуре. В связи с этим, принципиально важным в предложении Инициативы по ядерной угрозе (*Nuclear Threat Initiative*, *NTI)* является идея подготовки рекомендаций для высшего уровня военно-политического руководства по вариантам действий в конкретных ситуациях исходя из необходимости минимизации последствий любых ошибок со стороны системы управления.

Как представляется, набор таких рекомендаций применительно к разным возможным сценариям развития обстановки, может быть одинаковым не только для России и США, но и для всех ядерных государств. Однако маловероятно, что разработка таких сценариев осуществима только силами военных ведомств. Естественно, что варианты действий высшего уровня военно-политического руководства при возникновении критических ситуаций готовятся именно в Министерстве обороны, однако для военного руководства главным критерием при разработке рекомендаций всегда будет нанесение противнику, как минимум,

адекватного ущерба в любых условиях обстановки, а не сомнения в рациональности этих рекомендаций в случае каких-либо ошибок в системе управления. Поэтому подготовку рекомендаций по вариантам принятия решений на применение ядерного оружия в критических ситуациях целесообразно осуществлять в рамках совместных групп военных и гражданских специалистов.

Адекватность принятия военно-политическим руководством страны решения на применение ядерного оружия в значительной мере определяется не только достоверностью получаемой информации от СПРН и содержанием заранее подготовленных рекомендаций, но и надёжным обменом информацией при оценке обстановки между руководством Министерства обороны, президентом и другими лицами, участвующими в принятии решения [Blair B. 2019]. В зависимости от конкретной обстановки связь между должностными лицами может основываться на использовании каналов радиосвязи, в том числе и со стороны президента [12; 13]. Несмотря на закономерное отсутствие в открытой печати конкретной информации, есть все основания предполагать, что к используемому в этих средствах частотному диапазону всё больше приближаются частоты, используемые в перспективных сетях интернета и мобильной связи. Поэтому нельзя исключать возможных целенаправленных действий для нарушения устойчивости связи между должностными лицами, принимающими решение на применение ядерного оружия. Так, целью может быть провоцирование ядерного столкновение двух ведущих ядерных держав. При этом техническое обеспечение таких действий может основываться, например, на использовании находящихся на руках граждан мобильных телефонов, переводимых принудительно в режим активного излучения на заданных заранее (путём специальных закладок на стадии производства) частотах.

В этой связи представляется целесообразным рекомендовать принять меры по контролю средств, обладающих явными или неявными способностями к излучению в диапазоне частот работы средств специальной связи, используемых в процессе принятия решений. Перечень таких средств в определённой географической зоне необходимо минимизировать, а частотный диапазон должен подвергаться постоянному контролю и мониторингу.

ТЕХНИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ ОТ КИБЕРУГРОЗ ЭЛЕМЕНТОВ ОСНОВНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ЯДЕРНЫМ ОРУЖИЕМ

Первые образцы систем боевого управления ядерным оружием предусматривали реализацию алгоритмов обработки информации аппаратным способом. На участке контроля самих пусковых установок использовались аналоговые системы управления. В этот период киберугроз не существовало, и системы управления были неуязвимы. На последующих этапах развития широкое использование электронно-вычислительной техники, цифровых технологий подняло на

новый уровень проблему кибербезопасности. Поскольку кибероружие в значительной степени анонимно, оно может применяться практически из любой точки планеты, а реальный киберагрессор в течение длительного времени может оставаться неопознанным и ненаказанным. Всё большая сложность новых вооружений только увеличивает их уязвимость и ставит новые задачи перед проблемой кибербезопасости.

Особо остро стоит вопрос об аппаратных средствах и программном обеспечении, используемом при разработке и эксплуатации компонентов ядерного оружия и средств их доставки. Срок жизни элементной базы, особенно в жёстких условиях космоса, составляет единицы и редко десятки лет. Это тоже вопрос к кибербезопасности, потому что практически любую программу можно реализовать аппаратными средствами, но одними аппаратными средствами проблему кибербезопасности не решить. Покупка и применение импортных комплектующих привносит новые риски, связанные с наличием в них скрытых закладок. Тем не менее, использование программно-аппаратных средств при реализации небольших проектов очень эффективно. Что касается программных средств, впрочем, как и аппаратных, то все они должны пройти проверку на соответствие определённым требованиям – сертификацию.

В общем случае под сертификацией принято понимать независимое подтверждение соответствия тех или иных характеристик систем и средств заданным требованиям. В нашем случае речь идёт о программных средствах, в которых процедура сертификации призвана исключить возможность внесения закладок или преднамеренных ошибок в программное обеспечение на всех этапах его жизненного цикла.

Системы сертификации программ приняты как в России, так и на Западе. В России проблема сертификации возникла после распада СССР, когда появилась потребность в контроле безопасности при использовании зарубежного программного обеспечения, а также контроля качества российских программных систем, связанных с обработкой и защитой информации, относящейся к государственной тайне. Участниками процесса сертификации в то время стали в основном силовые ведомства и госструктуры.

На сегодняшний день, к сожалению, нет методов гарантированного выявления всех возможных уязвимостей программного обеспечения [Футтер Э. 2016]. Проведённая сертификация не исключает наличия в ней ошибок, связанных с недостаточным тестированием, либо намеренно сделанных в ней закладок разработчиками этих программ (операционных систем, трансляторов, компиляторов) или квалифицированными пользователями, знающими слабые места данной продукции. Это подтверждается большим количеством успешных хакерских атак на отечественные и зарубежные программы различного уровня. Все попытки многочисленных специализированных организаций препятствовать этим атакам пока не увенчались успехом.

Для России положение усложняется широким использованием зарубежных программ при разработке собственного программного обеспечения. Сертификация программ может производиться на функциональные возможности и на предмет наличия закладок. Проверка на функциональные возможности используется чаще всего при приёмке большинства отечественных программ. При соответствующем контроле на этапе разработки риск внедрения закладок в свои программы минимален.

Для сертификации зарубежных программ на наличие закладок необходимо знание исходных кодов этих программ. Но они могут отсутствовать, в том числе из-за намеренного нежелания предоставлять их разработчиком данных программ. В некоторых случаях возможна сертификация на наличие закладок с выездом специалистов к разработчику. Тогда сертификация должна осуществляться совместно с разработчиками программ. Но при появлении новой версии зарубежного продукта процесс сертификации необходимо повторять. Отсюда высокая стоимость этих работ и длительность процесса сертификации.

Работы по поиску закладок в миллионах исходных кодов очень трудоёмки. Поэтому даже в крупных программных и ответственных проектах, таких как миссия «Аполлон», где тестирование проводилось на высочайшем уровне, не удалось избежать программных ошибок. Такое же положение было с операционными системами ЭВМ единой серии (*IBM 360*) и других.

Проблемными являются требования по минимизации использования в системах боевого управления (СБУ) систем и средств двойного назначения, которые настолько переплетены между собой, что определить чёткую границу между ними не всегда возможно. Это в первую очередь системы энергоснабжения и связи, спутники, используемые одновременно в мирных и военных целях, в основном для сокращения расходов. Все они более подвержены угрозам кибератак, и любая из них может быть воспринята как попытка дестабилизировать СБУ и привести к катастрофическим последствиям.

Так что нельзя полностью исключать возможность разработки и внедрения программ, обеспечивающих резидентное нахождение на компьютере предполагаемого противника. В этом случае у противника появляется возможность отслеживать активность информационных систем и вывести их из строя в требуемый момент.

Таким образом нельзя исключать:

- применение ядерного оружия в результате кибератаки, достоверно имитирующей ядерную атаку со стороны предполагаемого противника;

- риск несанкционированного применения в результате кибератак в сочетании с физическими действиями для обхода мер обеспечения безопасности ядерных вооружений с целью хищения, либо несанкционированного применения ядерного оружия;

- несанкционированный приказ о применении ядерного оружия отданный злоумышленниками через взломанную систему управления;

- нарушение обмена по системам связи информацией, жизненно необходимой для принятия решения на применение ядерного оружия;

- внедрение вредоносного кода в один из компонентов ядерного оружия на этапе производства.

В России имеются операционные системы и пакеты прикладных программ, сертифицированные для использования в Министерстве обороны, других силовых структурах и в органах государственной власти. Это операционные системы различного назначения, системы управления базами данных, связью и другие прикладные программы, однако их количество и функциональные возможности *пока ограничены*. Тем не менее, в перспективе в сложившейся ситуации наряду с сертификацией необходимых зарубежных программ надо делать ставку на разработку и использование отечественного программного обеспечения. Существуют два подхода к созданию российских программ. Первый вариант предусматривает написание исходного кода с чистого листа. Учитывая, что реально работы по импортозамещению начались только с 2014 г., а также обострившиеся проблемы экономического развития, этот вариант очень длительный и затратный. Второй вариант предполагает создание национального программного обеспечения на основе доработки заимствованных исходных зарубежных кодов. Именно его и придерживаются российские компании.

КИБЕРЗАЩИТА СИСТЕМ БОЕВОГО УПРАВЛЕНИЯ ТАКТИЧЕСКИМ ЯДЕРНЫМ ОРУЖИЕМ РОССИИ И США

Прежде всего необходимо отметить, что ни в России, ни в США не существует отдельной системы управления тактическим ядерным оружием. Такое положение вполне логично. Как известно, право принятия решения на применение ядерного оружия, в том числе тактического, во всех ядерных государствах принадлежит только главам этих государств. Кроме того, тактическое ядерное оружие, как правило, до отдельного распоряжения хранится на складах. Вместе с тем со времён холодной войны к тактическому ядерному оружию было отношение как к реальному оружию «поля боя». Планирование применения ядерного оружия осуществлялось заблаговременно в рамках плана операций в интересах решения конкретных задач операций на театре военных действий. Соответственно и управление, в том числе ядерным оружием, осуществлялось в рамках существующей системы управления войсками на ТВД.

В период холодной войны главная задача ядерного оружия на ТВД состояла в отражении наступления противника в том случае, если с этой задачей не справились силы общего назначения. Но актуальной эта задача, учитывая соотношение сил общего назначения стран НАТО и вооружённых сил стран Варшавского договора, была именно для ВС НАТО. Фактически, основную роль в ядер-

ном сдерживании решали стратегические ядерные силы, а тактическое ядерное оружие лишь дополняло сдерживание, предотвращая угрозу возникновения и эскалации военного конфликта на региональном уровне.

Если бы ситуация оставалась такой же до настоящего времени, то проблема кибербезопасности системы управления тактическим ядерным оружием была бы неактуальной. Однако сегодня ситуация существенно изменилась.

С одной стороны, учитывая текущие отношения между Россией и Западом, может сложиться впечатление, что изменения носят лишь зеркальный характер. Если раньше было кардинальное превосходство за Объединёнными вооружёнными силами (ОВС) стран Варшавского договора, то теперь подавляющее военное превосходство у НАТО. На европейском ТВД теперь не НАТО, а Россия вынуждена опираться на потенциал ядерного сдерживания. Однако сама постановка вопроса о сравнении военной мощи одного государства с мощью военного альянса, куда входят почти 30 государств, одно из которых сохраняет статус самого мощного в мире, парадоксальна. Поэтому не выдерживают никакой критики предположения о возможности нападения России на одну или несколько стран НАТО.

Очевидно, что доктринальные документы должны быть ориентированы на все возможные варианты развития военного конфликта. В то же время есть общее понимание глобальных последствий ядерного конфликта с применением зарядов малой мощности даже в ограниченном регионе [14]. Исключать одиночных тактических ядерных ударов в интересах сдерживания эскалации военного конфликта с обычным оружием, к сожалению, нельзя, как и последующей эскалации применения ядерного оружия до неприемлемого масштаба.

В связи с изложенным, представляется, что главной целью киберзащиты для системы управления на ТВД является предотвращение применения ядерного оружия в неадекватной таким действиям ситуации. Достижение этой цели может осуществляться по двум основным направлениям:

- обеспечение военно-политического руководства страны достоверной, полной и объективной информацией по развитию обстановки на ТВД;

- сохранение за высшим военно-политическим руководством права принятия решения не только на первое применение ядерного оружия на ТВД, но и на каждое последующее его применение независимо от масштаба, в том числе при одиночных ударах.

Первое направление должно предусматривать не только предотвращение получения искажённой информации (дезинформации) с ТВД и от иных источников информации. Ядерное сдерживание может быть результативным и за счёт открытого информирования всех заинтересованных сторон в решимости использовать ядерное оружие и о конкретных шагах по подготовке к его приме-

нению. На этом этапе также очень важно обеспечить защиту информации от искажения и от вброса дезинформации.

Второе направление непосредственно связано с системой управления войсками на ТВД. Фактически должна быть предотвращена возможность использования тактического ядерного оружия в качестве оружия поля боя. Командующий войсками на ТВД не может иметь право после получения санкции на первое применение тактического оружия в дальнейшем использовать его по своему усмотрению. Каждое последующее применение должно быть санкционировано высшим военно-политическим руководством до тех пор, пока не будет принято решение о его полномасштабном использовании. Только после такого решения командующий на ТВД может применять находящееся в его распоряжении ядерное оружие по своим планам. Решение этой задачи не только связано с соответствующими алгоритмами функционирования системы управления войсками на ТВД, но и их защитой от кибератак.

ЗАКЛЮЧЕНИЕ: ВЫВОДЫ И РЕКОМЕНДАЦИИ

Рассмотренные проблемы кибербезопасности систем управления ядерным оружием России и США не могут претендовать на полноту, но тем не менее дают основание предложить несколько практических рекомендаций, которые могут снизить либо угрозы кибератак, либо их последствия. Так, представляется возможным рекомендовать:

1. Организовать Министерству обороны РФ совместно с Минобороны США прямое взаимодействие соответствующих структур, осуществляющих контроль космического пространства в целях своевременного обнаружения и нейтрализации угроз космическим аппаратам, в первую очередь, задействованных в контуре управления ядерным оружием. В последующем к такому взаимодействию привлечь Китай, учитывая создание им национальной СПРН и темпы развития космических систем.

2. России, США и Китаю провести согласование технических решений, критериев и алгоритмов, применяемых в национальных системах СПРН для определения факта пуска ракеты.

3. России и США реанимировать идею создания совместного Центра обмена данными от СПРН, уточнив задачи Центра в новых условиях. При уточнении таких задач особое внимание уделить привлечению к работе Центра представителей пяти ядерных государств, а также государств, обладающих ядерным оружием. Одновременно рассмотреть возможность в рамках расширенных задач этого Центра реализовать вероятность совместного мониторинга космического пространства в интересах обеспечения безопасности космических средств, задействованных в национальных системах СПРН, систем управления ядерным оружием, а также в интересах снижения уровня взаимной подозрительности и риска начала процесса вывода оружия в космос.

4. России и США рассмотреть теоретически возможные варианты ситуаций, способных привести к началу процесса выработки решения на применения ядерного оружия и на этой основе внести изменения в действующие варианты решений президентов с учётом приоритета минимизации риска ошибочных решений на применение ядерного оружия. По мере возможности на рабочем уровне руководителей военных ведомств провести согласования принятых подходов.

5. России и США по мере дальнейшего распространения действия коммерческих систем связи вблизи диапазона частот средств конференцсвязи, используемых при выработке решения на применение ядерного оружия обратить внимание на предотвращение появления средств мобильной связи со скрытыми возможностями излучения на частотах работы упомянутых средств связи.

6. Рост сложности систем боевого управления требует тщательной отработки алгоритмов работы элементов этой системы. В связи с этим, наряду с повышением надёжности аппаратных средств реализации алгоритмов работы, при разработке программ повысить внимание к качеству сертификации (тестирования) программных продуктов, определяющему в конечном счёте надёжность функционирования программ при реализации алгоритмов управления.

7. В системах управления войсками на ТВД на алгоритмическом уровне предусмотреть исключение возможности после получения приказа на первое применение ядерного оружия использовать его командующему войсками на ТВД по своему усмотрению.

ИСТОЧНИКИ

1. National Security Strategy of the United States of America. December 2017. The White House. Washington, DC. Available at: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed 20.06.2020).

2. Defense Space Strategy Summary June 2020. Available at: http://spaceref.com/news/viewsr.html?pid=53780 (accessed 20.06.2020).

3. The National Strategy to Secure Cyberspace Available at: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (accessed 20.06.2020)/

4. International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World, Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed 23.06.2020).

5. National Cyber Strategy of the United States of America https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (accessed 23.06.2020)

6. Основы государственной политики РФ в области ядерного сдерживания Available at: http://kremlin.ru/acts/news/63447 (accessed 20.06.2020)

7. Система «Периметр» или «Мертвая рука»: для чего создавалась машина судного дня и как она отразит ядерную атаку. Available at: https://www.kp.ru/putevoditel/interesnye-fakty/sistema-perimetr-ili-mertvaya-ruka/ (accessed 20.06.2020).

8. The RAMOS (Russian-American Observation Satellite) Program. Available at: https://www.drewexmachina.com/the-ramos-russian-american-observation-satellite-program (accessed 20.06.2020).

9. Закрытие проекта РАМОС. Available at: https://lenta.ru/news/2004/02/13/ramos/ (accessed 20.06.2020).

10. Space-X. Available at: https://www.rbc.ru/rbcfreenews/5e31b3389a794761ff97be2e (accessed 20.06.2020).

11. Nuclear Weapons in the New Cyber Age-Russian, NTI, 2018. Available at: https://www.nti.org/analysis/reports/nuclear-weapons-cyber-age (accessed 25.06.2020).

12. Ядерный чемоданчик США. Available at: https://ru.wikipedia.org/wiki (accessed 25.06.2020).

13. Ядерный чемоданчик России. Available at: https://ru.wikipedia.org/wiki (accessed 25.06.2020).

14. An India-Pakistan Nuclear War Could Kill Millions, Threaten Global Starvation, by CBRNE Central Staff. November 15, 2019. Available at: https://cbrnecentral.com/an-india-pakistan-nuclear-war-could-kill-millions-threaten-global-starvation/20766/ (accessed 25.06.2020).

СПИСОК ЛИТЕРАТУРЫ

Роговский Е.А. 2014. Кибер-Вашингтон: глобальные амбиции. М.: Международные отношения. 848 с.

Футтер Эндрю. 2016. Ядерное оружие в век информационных технологий. *Россия в глобальной политике.* №6 (https://www.globalaffairs.ru/articles/yadernoe-oruzhie-v-vek-informaczionnyh-tehnologij).

Ярынич В. 2002. Система управления стратегическими ядерными силами США. Центр по изучению проблем контроля над вооружениями, энергетики и экологии. СНВ-сайт. 14 декабря 2002 (https://www.armscontrol.ru/start/rus/basics/us-c3-21.htm)

REFERENCES

Bruce G. Blair. 2019. Loose cannons: The president and U.S. nuclear posture. Available at: https://doi.org/10.1080/00963402.2019.1701279 (accessed 26.06.2020).

Rogovsky Ye.A. 2014. Cyber-Washington: global ambitions. Moscow. Mezhdunarodniye otnosheniya. P.848.

Futter A. 2016. Nuclear weapons in the century of information technologies. Available at: https://www.globalaffairs.ru/articles/yadernoe-oruzhie-v-vek-informaczionnyh-tehnologij (accessed 26.06.2020).

Yarinich V. 2002. System for the command and control of the strategic nuclear forces of the USA. Center for Arms Control, Energy and Environmental Studies. STAR-site. 14.12.2002. Available at: https://www.armscontrol.ru/start/rus/basics/us-c3-21.htm (accessed 26.06.2020).

ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

ЗОЛОТАРЁВ Павел Семёнович, кандидат технических наук, ведущий научный сотрудник Института США и Канады Российской академии наук (ИСКРАН).

Российская Федерация, 121069 Москва, Хлебный пер., 2/3.

Pavel S. ZOLOTAREV, Candidate of Science (Technical), Leading Researcher, Institute for the U.S. and Canadian Studies, Russian Academy of Sciences (ISKRAN)

2/3 Khlebny per., Moscow 121069, Russian Federation.