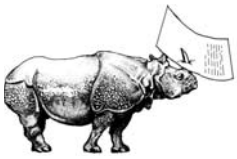


Олег Демидов

КИБЕРКОМАНДОВАНИЕ США: УРОКИ ДЛЯ РОССИИ

*

В последнее время в российских вооруженных силах резко ускорилась работа по киберугрозам, остававшаяся едва ли не единственным *белым пятном* в течение предыдущих лет. В январе 2012 г. в открытом доступе появился документ Минобороны с витиеватым названием[1] — по сути, первый прообраз доктрины действий ВС РФ в условиях информационной войны.

В «Концептуальных взглядах...», в частности, отражен болезненный для России опыт *пятидневной войны* 2008 г. — впервые заданы приоритеты информационного освещения и сопровождения конфликтов, прописаны задачи взаимодействия ВС с медиа и общественностью. Дальше — больше: в марте 2012 г. вице-премьер Д. О. Рогозин, ответственный за оборонный комплекс, объявил о скором создании в России собственного киберкомандования. Причем за образец для него предлагается взять киберкомандование Соединенных Штатов (U. S. CYBERCOM), что будет означать резкий отход от двух важных тенденций прежних лет.

Первая из них — приоритет угроз, связанных с социально-политическими аспектами информационной войны, то есть исходящих от информации как таковой, контента (при серьезном отставании в оценке вызовов кибербезопасности в узком смысле, то есть устойчивости и защищенности компьютерных сетей). Вторая — практически полное доминирование в вопросах информационной безопасности спецслужб (ФСБ, ФСО, Федеральной службы по техническому и экспортному контролю), притом что напрямую в спектр задач Минобороны эти вопросы де-факто не входили.

Подтверждением того, что за укрепление военно-стратегического киберпотенциала России решено взяться всерьез, стало создание Фонда перспективных исследований — некоммерческой структуры для содействия прорывным разработкам в сфере ВПК, которую сразу стали сравнивать с американской DARPA. Директором Фонда в феврале 2013 г. стал бывший сотрудник ФСТЭК Андрей Григорьев. Весь цикл создания фонда от первого объявления о нем в январе 2012 г. до формирования его структуры, утверждения бюджета в размере до 3 млрд рублей и назначения руководства прошел всего за год, что очень быстро по российским меркам.

На этом фоне почти незамеченным остался тот факт, что 17 октября 2012 г. Минобороны совместно с Агентством стратегических инициатив, Министерством образования и науки РФ и МГТУ им. Н.Э. Баумана объявило всероссийский конкурс научно-исследовательских работ, одна из тем которого — *Методы и средства обхода антивирусных систем, средств сетевой защиты, средств защиты ОС*[2]. Как следует из названия темы и комментариев российских экспертов, речь может идти, в том числе, и о разработке боевых наступательных вирусов для преодоления защитных систем вероятного противника[3].

Подобная постановка вопроса кардинально расходится с сугубо оборонительной стратегией в сфере *информационного противоборства*, которая прописана в Военной доктрине РФ от 2010 г., а также во внешнеполитических российских инициативах. О сдвиге в направлении проактивной деятельности в киберпространстве говорит и возросшая активность по формированию новых (полу)секретных структур, ответственных за информационную безопасность, в составе Минобороны — 13 февраля 2013 г. было объявлено о создании такой структуры в Генштабе ВС РФ.

Однако лихорадочная активность военных вовсе не говорит о том, что спецслужбы *сдают им пост*. Несмотря на растущее внимание Минобороны к киберугрозам военно-стратегического характера, именно ФСБ, ФСО и ФСТЭК сохраняют за собой приоритетную роль в вопросах разработки единой и полноохватной системы кибербезопасности в РФ.

Спустя несколько дней после раскрытия *Лабораторией Касперского* кибершпионской сети *Red October*, 15 января 2013 г. Владимир Путин подписал указ № 31с, который возлагает на ФСБ РФ создание общенациональной государственной системы, призванной обеспечить полный цикл предупреждения и противодействия кибератакам на российские компьютерные сети, включая прежде всего критическую инфраструктуру. Именно это решение некоторые представители экспертного сообщества считают поворотной точкой в российской политике информационной безопасности.

В то же время инициатива конца 2012 г. по разработке комплексной российской стратегии кибербезопасности, выдвинутая сенатором Русланом Гаттаровым[4], воспринимается как существенно менее приоритетное направление по той причине, что Совет Федерации сам по себе не имеет необходимого аппаратного веса и не обладает неформальным правом на *определение подходов* в этой чувствительной области.

Любопытно, что параллельное продвижение вопросов кибербезопасности по двум ветвям госаппарата (военные и спецслужбы) уже угрожает обострить их доселе латентное соперничество за полномочия. Этот процесс может проявиться в полной мере в ближайшие месяцы по мере выработки решения об окончательном облике и структуре российского киберкомандования.

С одной стороны, идея создания в России аналога американского *Киберкома* доказала свою исключительную востребованность для Минобороны, оказавшись одним из немногих проектов эпохи А. Э. Сердюкова, который получил полную поддержку нового министра обороны С. К. Шойгу. В середине февраля 2013 г. стало известно, что процесс формирования облика перспективной военной структуры должен завершиться уже в нынешнем году, причем, скорее всего, она станет главным управлением военного ведомства или командованием отдельного рода войск (наряду с РВСН и ВДВ).

Опыт США как ведущей мировой кибердержавы говорит о целесообразности разведения функций спецслужб и вооруженных сил в структурно-организационном плане. Киберкомандование США решает задачи наряду с ЦРУ, министерством внутренней безопасности, агентством национальной безопасности и рядом других структур. В то же время синергия военных и спецслужб необходима для борьбы с киберугрозами. Любопытной практикой в этом плане является совмещение одним лицом руководящих постов в ведомствах с частично пересекающимися задачами — так, нынешний руководитель *Киберкома* Кит Александер одновременно является директором АНБ и центральной службы безопасности. Подобные решения вполне возможны и в России в качестве части политико-административного маневрирования в сфере кибербезопасности.

В целом, 2013 и 2014 гг. с большой долей вероятности станут для российского курса в области кибербезопасности решающим периодом, на протяжении которого оформятся внешние контуры и новые доктринальные основания государственной

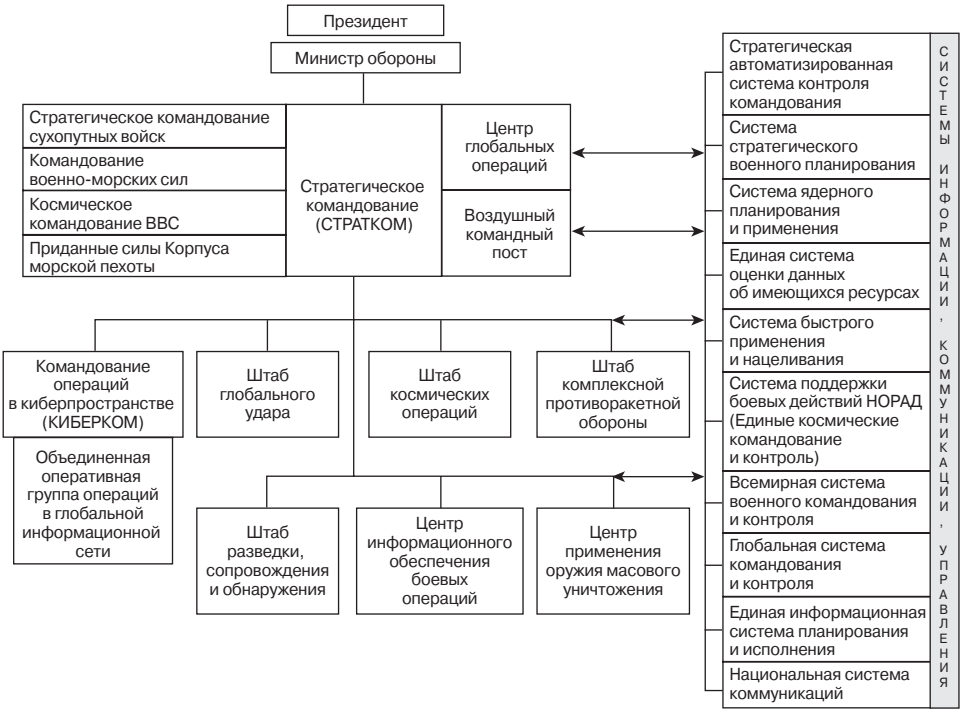
политики, а также будет дан старт новым долгосрочным программам и проектам. Период трансформации государственной политики в области информационной безопасности, из которой выделяется самостоятельное направление борьбы с киберугрозами, означает наличие *окна возможностей* для зарубежных партнеров РФ, а также всех общественных групп, которые заинтересованы в том, чтобы перспективный курс в отношении киберпространства отвечал их интересам.

В то же время для самой России этот временной горизонт является и *окном уязвимости*, в течение которого нехватка отработанных практик реагирования на эволюционирующие вызовы в киберпространстве будет представлять повышенный риск для национальной и общественной безопасности. Политика кибербезопасности в России вступает в *кризис роста* — естественно рискованный этап ее развития.

В этих условиях для российских военных может быть любопытен опыт модели киберкомандования Соединенных Штатов при формировании его отечественного аналога. В частности, он позволяет проследить историю непростых дебатов о том, на каком уровне следует выделять и обособлять повестку кибербезопасности в спектре задач вооруженных сил — что сейчас необходимо сделать и России.

Несмотря на свое название, американское киберкомандование, сформированное в июне 2009 г., не является одним из объединенных боевых командований ВС США, а находится в подчинении стратегическое командования, ответственного, в том числе, за использование американских стратегических ядерных сил.

Военные аспекты кибербезопасности выдвинулись в число главных приоритетов Пентагона к середине первого президентского срока Дж. Буша-младшего, с того же времени между американскими спецслужбами и самими военными структурами началась жесткая конкуренция за полномочия в этой сфере. Тогда же возникла идея создания объединенного киберкомандования, которое полностью замыкало бы на себе обеспечение всей деятельности военных



Чтобы быть в курсе ключевых событий в области информационной безопасности и управления интернетом, подписывайтесь на электронный бюллетень Пульс Кибермира: http://www.pircenter.org/mailouts

в киберпространстве. Однако общий отказ американских военных от узкой специализации сыграл против этого. Кроме того, у Пентагона тогда не было ни понимания, ни проработанных планов совместной деятельности видов войск в условиях кибервойны, как и однозначного определения самого этого термина.

Поэтому общая ответственность за проблематику кибервойн и была делегирована Страткому, однако фактическое осуществление боевых операций в сетях было возложено на военно-воздушные силы. В дальнейшем эта тенденция получила развитие: в 2007 г. было создано киберкомандование ВВС США, просуществовавшее в предварительном статусе до конца 2008 г., после чего его функции были переданы Космическому командованию военно-воздушных сил.

Особая роль ВВС в вопросах стратегической кибербезопасности отражала давнюю традицию, уходящую корнями еще к началу 1990-х гг., когда успех операции *Буря в пустыне* был во многом обусловлен применением *умного вооружения* и использованием информационно-компьютерных технологий прежде всего именно авиационными соединениями. 10 сентября 1993 г. был создан центр информационных боевых действий ВВС; цели его включали расширение возможностей информационного оружия на основе опыта иракской кампании.

Оттуда же проистекает и мощный крен на наступательные и превентивные меры, усиленный при Дж. Буше-младшем и разделяемый нынешними *киберстратегами* Пентагона. К 2007–2008 гг. активность представителей военно-воздушных сил достигла апогея; их риторику хорошо обобщает следующий афоризм: «Если вы защищаетесь в киберпространстве, вы уже проиграли».

Столь явное доминирование ВВС вызвало неприятие в структурах других видов и родов войск. После долгих дискуссий и аппаратных маневров к 2009 г. американские военные верхи пришли к пониманию того, что создание некоей универсальной структуры, которая обеспечит взаимодействие и интеграцию функций основных видов и родов войск, неизбежно. В противном случае параллельное развитие киберкомпетенций ВВС, ВМФ и сухопутных сил повлекло бы разрыв в стратегии, тактике, а также совокупном киберпотенциале. Как следствие это привело бы к потере качества взаимодействия различных видов и родов войск, а также возможности их оперативной совместимости.

Здесь же возникли вопросы кибероборонны, обнажив фундаментальный недостаток сугубо *наступательного* подхода, обусловленный растущей *уязвимостью* США в киберпространстве, основанной на зависимости всех отраслей американского хозяйства и управления (включая национальную оборону) от компьютерных сетей. В итоге 23 июня 2009 г. было основано киберкомандование в составе Страткома. Так была решена *большая дилемма*, связанная с необходимостью определения системы координат кибервойны в спектре задач различных структур вооруженных сил.

Российское военное руководство решает аналогичную задачу сейчас, пока статус *базового уровня* российской военной киберструктуры не определен и плавает в широком диапазоне от главного управления Минобороны до командования отдельного рода войск. Проводя весьма условные параллели, можно сказать, что первый вариант примерно соответствует киберкомандованию США в его нынешнем виде, в то время как второй обещает серьезную доктринальную новацию в российских Вооруженных силах.

Создание же отдельного рода *информационных войск* в России поставит их на один уровень с железнодорожными войсками, ВДВ и РВСН. Столь резкое повы-

шение статуса вопросов информационной безопасности для российской армии пока преждевременно в силу дефицита необходимых ресурсов: доктринальной и тактической базы, материальной инфраструктуры, финансов и, самое главное, квалифицированных кадров, ориентирующихся в вопросах угроз из киберпространства.

Россия, несмотря на резко возросшую активность в этой сфере, только сейчас проходит американскую траекторию 2007–2009 гг. Это значит, что американский опыт в выстраивании национальной системы кибероборонs еще не устарел и, по крайней мере, отчасти релевантен для РФ, коль скоро военное руководство ориентируется именно на опыт *Киберкома*. Но, как минимум, одно радикальное отличие уже имеется — более низкая степень зависимости национальной критической инфраструктуры от кибертехнологий и внимание именно вопросам обороны в киберпространстве.

Примечания

[1] Концептуальные взгляды на деятельность Вооруженных сил Российской Федерации в информационном пространстве. Министерство обороны Российской Федерации. ens.mil.ru/files/morf/Strategy.doc (последнее посещение — 13 февраля 2013 г.)

[2] Всероссийский конкурс научно-исследовательских работ среди граждан Российской Федерации в интересах Вооруженных сил Российской Федерации. Министерство обороны Российской Федерации. 2012, 17 октября. http://ens.mil.ru/education/contests/more.htm?id=1719@morfSimpleEvent (последнее посещение — 15 февраля 2013 г.)

[3] Минобороны объявило тендер на наступательное кибероружие. *Взгляд*. 2012, 18 октября. http://vz.ru/news/2012/10/18/603077.html (последнее посещение 15 февраля 2013 г.).

[4] Совет Федерации создает комиссию по кибербезопасности. Известия. 2012, 20 декабря. http://izvestia.ru/news/541923 (последнее посещение — 15 февраля 2013 г.)