постоянного доступа к этим системам означает наступление «Фазы 3», ключевым словом в характеристике которой является доминирование. Как сказано в документах Эдварда Сноудена, в этой фазе предусмотрен целенаправленный контроль/уничтожение критически важных систем и сетей посредством ранее обеспеченного в «Фазе 0» доступа. Критически важными для АНБ являются инфраструктуры, обеспечивающие функционирование общества: энергетическая, телекоммуникационная, транспортная и финансовая.

В одной из подготовленных АНБ презентаций НАТО утверждается, что следующий крупный международный конфликт начнется в киберпространстве. Ориентируясь на эти перспективы, правительство США наращивает мощь военных киберподразделений. В бюджете спецслужб на 2013 год для АНБ на проведение спецопераций в интернете предусматривался $1 млрд, а на финансирование так называемых «нестандартных решений» — $32 млн дополнительно.

Как сообщает Washington Post, Соединенные Штаты направляют все возможные усилия на разработку нового поколения кибероружия, которое будет способно нарушать корректную работу компьютерных систем противников, даже если они не подключены к интернету. В 2011 году на ускорение темпов разработки кибероружия и оборонных технологий ведущему научно-исследовательскому агентству Пентагона DARPA (Defense Advanced Research Projects Agency) было выделено $500 млн на пять лет. Агентство DARPA объявило о новых инициативах в области развития кибероружия, в том числе об «ускоренной» программе. «Наши кибердействия должны быть быстрыми и масштабными»,— заявляют представители DARPA.

В Пентагоне отмечают, что кибероружие должно соответствовать темпам развития информационных технологий и угроз. Чиновники планируют разрабатывать технологии, которые используют радиосигналы для встраивания кодов в компьютерные системы удаленно. Стоит отметить, что DARPA намерено нацелить большую часть исследований на решение именно таких военно-специфических вопросов.

«Госструктуры США, включая АНБ, посредством разного рода государственных программ тесно сотрудничают с крупнейшими национальными и транснациональными компаниями—производителями микроэлектроники и программного обеспечения,— рассказывает Игорь Жуков, заместитель генерального директора по защищенным радиоэлектронным информационным технологиям концерна „Радиоэлектронные технологии“ (входит в госкорпорацию „Ростех“).— Суть данного сотрудничества состоит в предоставлении спецслужбам США несанкционированного доступа к информации, обрабатываемой на аппаратных и программных платформах. То есть в свои продукты производители внедряют специальные возможности, так называемые back doors, или закладки, которые позволяют получать доступ к информации в обход встроенных механизмов защиты (например, программа Bullrun)». По словам эксперта, в свою очередь, государственные структуры США оказывают поддержку продвижению на мировых рынках продукции вступивших в «программу» компаний. «В частности, в СМИ неоднократно проходила информация о поставках США ряду государств связного и криптографического оборудования в кредит на льготных условиях либо вообще бесплатно. Также проходила информация об акциях активного продвижения такого оборудования, осуществляемого непосредственно сотрудниками Госдепартамента и МО США»,— добавляет Игорь Жуков.

МЯГКИЙ ЩИТ В новой военной доктрине, утвержденной президентом РФ в конце декабря 2014 года, среди основных внешних военных опасностей также отмечается массированное использование информационных и коммуникационных технологий в военно-политических целях. Поэтому новая госпрограмма вооружений ставит своей целью создание эффективных информационно-управляющих систем ВВСТ, защищенных от возможных кибератак.

В феврале 2015 года главой Минобороны России была подписана «Концепция развития информационных и телекоммуникационных технологий вооруженных сил на период до 2020 года». В концепции также содержатся ответы на изменения в военной науке в сфере развитых информационных технологий и информационного управления. В марте было принято решение о создании Совета по кибербезопасности. На совещании по вопросам информационной безопасности в марте в МГУ им. М. В. Ломоносова вице-премьер Дмитрий Рогозин заявил, что в России появится своя собственная система противодействия киберугрозам. Она будет основана на применении «умного» оружия, которое производится «с помощью сложнейших производственных линий и технологических цепей». Сейчас формируется «новая программа вооружений с использованием такого умного оружия».

В указанных документах и заявлениях руководителей страны отмечаются как источники информационных угроз (сильная в отношении возможных кибератак страна, страна, равная по силе, слабый противник в виде организованной преступной или террористической группы), так и особенности современных военных и иных конфликтов противоборствующих сторон, где составляющая информационных воздействий играет не последнюю роль.

Особенно сильно эта роль проявляется в ходе проведения новой стратегии «нелинейного ведения войны» в виде гибридной или «мягкой» войны. В ее арсенале присутствуют информационная война или информационные воздействия, как правило предшествующие военной операции или идущие параллельно и включающие информационно-психологическую (дезинформация, пропаганда, использование протестного потенциала населения противника и др.), а также информационно-техническую составляющую (кибератаки и др.) на основные управляющие и организационно-технические системы противника. Такого же определения гибридной войны придерживается и руководство НАТО, которое в этом качестве подразумевает подход, сочетающий «конвенциональные военные действия» и новые сложные кампании по «пропаганде и дезинформации».

«Понятно, что все эти формы ведения гибридной войны начинают использоваться одной из сторон зарождающегося и идущего конфликта тогда, когда нецелесообразно и невыгодно масштабное силовое противостояние со всеми вытекающими последствиями. Уже сейчас начало массового применения кибератак на другое государство в ряде стран НАТО может рассматриваться как повод для применения статьи о коллективной обороне»,— поясняет Игорь Жуков.

ПОДНЕБЕСНЫЕ ЦЕЛИ Международные эксперты называют российские киберинструменты и методы более умелыми, а китайские — более масштабными. Впрочем, руководство Китая всегда отвергает причастность к любым инцидентам, связанным с нападениями на западные страны, в первую очередь на США. При этом косвенное доказательство причастности Китая к ведению кибервойн обнаружилось в официальном отчете Народно-освободительной армии Китая (НОАК). О том, что Китай признает существование кибервойск в составе своей армии, говорится в тексте публикации «Наука военной стратегии» (The Science of Military Strategy). Документ готовился ведущими исследовательскими институтами совместно с НОАК и содержит детальный анализ военной стратегии Поднебесной. Согласно отчету, в Китае действует три вида кибервойск.

Первый — это военные специалисты в сфере сетевой безопасности. Они действуют по военным принципам. Их задача — организация кибератак и защита от них. Второй — специальные группы, действующие внутри спецслужб, таких как Министерство государственной безопасности и Министерство общественной безопасности. Третий вид — группы независимых хакеров, которых можно быстро мобилизовать для совершения информационных операций.

Специалисты отмечают, что, по всей видимости, все три группы работают в тесном контакте и подчиняются руководству НОАК. Кроме того, в последнем издании энциклопедии «Наука военной стратегии», выпущенном НОАК на родном языке и представляющем собой «лучшее пособие по китайской военной машине», сообщает The Daily Beast, также говорится о том, что в Китае существуют кибервойска, в задачи которых входит не только защита, но и нападение на сети иностранных государств. В последнем издании военной энциклопедии Китая прямо сказано о наличии у государства специальных хакерских группировок. Вооруженные силы Китая располагают специальными подразделениями, осуществляющими кибератаки на вычислительные сети иностранных государств. Согласно энциклопедии, в Китае существуют два подразделения с хакерами. Одно — при вооруженных силах, второе — при разведывательных службах. Кроме того, существуют некие неправительственные «внешние группировки». Они могут быть организованы и мобилизованы по необходимости, приводит выдержки из энциклопедии The Daily Beast.

Впрочем, пока для России Китай больше партнер, чем угроза. 9 мая правительства стран подписали пакт о ненападении друг на друга в киберпространстве. Международные эксперты назвали соглашение уникальным. Также РФ и Поднебесная договорились обмениваться данными о киберугрозах и технологиями.

Прошло лишь пять лет с момента появления первой «кибербоеголовки», за это время правительства разных стран обзавелись кибервойсками и признали, что «мягкая» война уже идет полным ходом, пока мы читаем эту статью на сайте, изучаем ленту в Facebook и играем в «Злых птиц» на iPhone. О таких битвах сложно рассказывать живописно и невозможно снять шокирующий фоторепортаж, но их последствия могут оказаться еще более разрушительными, чем взрыв ядерной бомбы. ■

«ГИСП — ЭТО ПРЕЖДЕ ВСЕГО ИСТОЧНИК ДАННЫХ ДЛЯ ПРИНЯТИЯ РЕШЕНИЙ КАК ПРАВИТЕЛЬСТВОМ РФ, ТАК И СУБЪЕКТАМИ ПРОМЫШЛЕННОСТИ»

Министерство промышленности и торговли РФ начало реализацию глобального проекта по созданию Государственной информационной системы российской промышленности (ГИСП). О ходе решения этой задачи „Ъ“ рассказал первый заместитель министра промышленности и торговли России ГЛЕБ НИКИТИН.

BUSINESS GUIDE: Насколько, на ваш взгляд, важна роль государства в поддержке развития ИТ-технологий в индустриальном секторе?

ГЛЕБ НИКИТИН: Не открою большого секрета, сказав, что за ИТ-технологиями будущее современной промышленности, поэтому Минпромторгом уделяется повышенное внимание вопросам информатизации. Например, в рамках программы создания и поддержки инжиниринговых центров мы разработали механизм по возмещению части затрат на приобретение специализированного программного обеспечения. В 2014 году благодаря этим мерам поддержки компании малого и среднего бизнеса, осуществляющие деятельность в сфере инжиниринга и промышленного дизайна, имели возможность приобретать необходимое ПО со скидкой до 75%. Общий размер предоставленной скидки на ПО составил 140 млн руб.

BG: Насколько сегодня актуальна задача по импортозамещению в области программных продуктов для российского индустриального сектора?

Г. Н.: Импортозамещение в сфере ИТ-технологий мы считаем крайне важной задачей, особенно в условиях введения Западом антироссийских санкций. Здесь на первый план выходит уже не столько экономическая выгода, сколько вопросы безопасности. К сожалению, в настоящее время доля российских разработок в ИТ-области невелика. Мы понимаем, что переход на отечественные разработки — процесс длительный, сложный и требующий больших инвестиций, но со временем мы ожидаем прогресса в этом направлении. Например, в план мероприятий по импортозамещению мы включили продукцию радиоэлектронной промышленности, куда входят в том числе вычислительная техника, телекоммуникационное оборудование, периферийное оборудование, электронная компонентная база и прочее. Мы ожидаем, что развитие электроники поможет стимулировать развитие собственных ИТ-технологий.

BG: Для чего создается Государственная информационная система российской промышленности?

Г. Н.: Мы рассматриваем ГИСП прежде всего как источник данных для принятия решений как для правительства РФ, так и для самих субъектов промышленности. Это новый инструмент промышленной политики. Единый центр по сбору данных и их диагностике в сфере промышленности позволит нам сформировать полную информационную картину планов и потребностей российских промышленных предприятий, даст разбивку по регионам, исключит дублирование запросов и межотраслевой дисбаланс. По сути, ГИСП представляет собой единое окно, включающее в себя весь массив нормативно-правовых актов в сфере промышленности, горячую линию поддержки, открытый каталог потенциальных промышленных площадок и т. д. Система предусматривает исключительно электронный сбор информации.

BG: В каком виде предстанет ГИСП для конечного пользователя?

Г. Н.: Это будет интернет-портал, через который конечные пользователи смогут воспользоваться необходимыми сервисами, зарегистрировав свой личный кабинет. Внутреннее ядро будет включать в себя технологическую платформу и необходимую инфраструктуру для сбора, обработки и хранения данных.

BG: С какими данными пользователи смогут работать через ГИСП?

Г. Н.: ГИСП позволит пользователям получить сведения о состоянии промышленности и прогнозе ее развития, о субъектах деятельности в сфере промышленности, о прогнозах выпуска основных видов промышленной продукции и об их фактическом выпуске, об объемах импорта промышленной продукции в Россию, а также данные об использовании ресурсосберегающих технологий и возобновляемых источников энергии. Кроме того, сюда будет поступать информация о государственных и муниципальных промышленных программах, о мерах стимулирования промышленности, о показателях эффективности этих мер и о кадровом потенциале. И, наконец, в ГИСП будут выгружаться ежегодные доклады о состоянии и развитии промышленности.

BG: Чем руководствовался Минпромторг, включая этот проект в свой план работы?

Г. Н.: Задача по созданию ГИСП появилась при разработке нами законопроекта «О промышленной политике». Сам закон был принят 31 декабря 2014 года и вступает в силу 1 июля 2015 года. Правительство РФ обязало наше министерство разработать и утвердить требования к ГИСП и наделило нас полномочиями обладателя информации, содержащейся в данной системе.

BG: Как будет наполняться ГИСП, каковы источники информации?

Г. Н.: Для наполнения системы данными промышленные предприятия, органы государственной власти, местного самоуправления и другие субъекты деятельности в сфере промышленности должны будут обеспечить Минпромторгу доступ к своим базам данных посредством единой системы межведомственного электронного взаимодействия. Часть данных, размещенных в ГИСП, будет открыта и опубликована в интернете в разделе «Открытые данные» официального сайта нашего министерства.

BG: Каким образом посредством ГИСП предполагается выстраивание системы отраслевых балансов в промышленности?

Г. Н.: Действительно, до сих пор остается актуальной проблема отсутствия межотраслевых балансов в стране, что зачастую приводит к созданию искусственных профицитов промышленных мощностей в разных регионах. В настоящее время данные, необходимые для анализа и принятия решений, разрозненны и к ним не всегда имеется доступ. Предполагается, что в единой системе они будут аккумулированы и это позволит снять проблему.

BG: На каком этапе сегодня находится реализация этого проекта, какова его предварительная стоимость?

Г. Н.: На данном этапе реализации этой задачи уже завершено общественное обсуждение проекта соответствующего постановления правительства РФ, и сейчас документ проходит этап антикоррупционной экспертизы. Начало работы ГИСП можно ожидать уже в 2016 году. По предварительным расчетам, на реализацию первого этапа потребуется около 47 млн руб., в ноябре 2015 года будет объявлен конкурс.

Интервью взяла МАРИЯ АНАСТАСЬЕВА