«ДЕЛО HUAWEI» КАК ПРИМЕР РЕАЛИЗАЦИИ ГИБРИДНОЙ УГРОЗЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В ВЫСОКОТЕХНОЛОГИЧНОЙ СФЕРЕ ПРИ ЭКСПЛУАТАЦИИ АСУП

Гриняев Сергей Николаевич
Д.т.н., с.н.с., РГУ нефти и газа (НИУ) имени И. М. Губкина
Панкратенко Игорь Николаевич
Д.и.н., заместитель генерального директора, АНО «Центр стратегических оценок и прогнозов» (Москва)
Медведев Дмитрий Андреевич
К.полит.н., доцент, РГУ нефти и газа (НИУ) имени. И. М. Губкина
Medvedev.d@gubkin.ru
Каширин Дмитрий Игоревич
Аспирант, РГУ нефти и газа (НИУ) имени И. М. Губкина

Аннотация. В статье рассмотрены вопросы трансформации угроз национальной безопасности в условиях развития глобальной цифровой среды. Отмечено, что процессы обеспечения комплексной безопасности должны быть интегрированы в процессы на всех уровнях функционирования и развития объекта. На примере «дела Huawei» авторы иллюстрируют модернизацию методов противоборства на межгосударственном уровне.

Ключевые слова: цифровизация, гибридные угрозы, комплексная безопасность, Huawei.

"HUAWEI CASE" AS AN EXAMPLE OF HYBRID THREAT REALIZATION TO THE NATIONAL SECURITY IN HIGH-TECH SPHERE IN THE OPERATION PROCESS CONTROL SYSTEM

S. Grinyaev
I. Pankratenko
D. Medvedev
D. Kashirin

Summary. The article deals with the transformation of national security threats in the context of the global digital environment. It is noted that the processes of complex security should be integrated into the processes at all levels of operation and development of the object. On the example of "Huawei case" the authors illustrated the modernization of methods of confrontation at the intergovermental level.

Keywords: digitalization, hybrid threats, complex security, Huawei.

В условиях активной цифровизации глобального информационного пространства объекты обеспечения национальной безопасности все чаще подвергаются угрозам, которые носят гибридный, комплексный, многовекторный характер (экономические санкции, отказ в доступе к технологиям, инициирование компьютерных атак и др.).

Характерной чертой таких угроз является то, что они зарождаются в одной сфере, а реализуются в другой или нескольких сферах безопасности. Это приводит к масштабной трансформации подходов к обеспечению безопасности, так как, например, защита информации до недавних пор рассматривалась как отдельное направление обеспечения безопасности, не связанное с обеспечением устойчивости и качества управления в системе в целом [1].

В этих условиях изменяется и организационная структура обеспечения безопасности [2]. Процессы обеспечения комплексной безопасности должны быть интегрированы в процессы на всех уровнях функционирования и развития объекта.

Появление новых угроз для различных видов безопасности, безусловно, связано с усложнением механизмов управления. Так, например, использование в системах управления «цифровые двойников» приводит к появлению нового, ранее неидентифицированного вида угроз безопасности [3]. Новые угрозы выходят за рамки классической триады «конфиденциальность, целостность, доступность» [4]. В частности, возникает комплексная угроза несоответствия модели объекту.

Формирующаяся информационная цифровая среда создает предпосылки для изменения доминирующих социально-экономических моделей. И, если на индустриальном этапе развития характерны централизация и концентрация производства, то для информационного этапа конкурентным преимуществом становится гибкая децентрализованная организация управленческих процессов в социально-экономической сфере [5].

Как отмечают теоретики глобального информационного общества, управлять социально-экономическими процессами эффективно могут только институциализированные субъекты, которые обладают большей информацией и имеют возможность регулировать поток и каналы ее распространения [6].

В качестве примера реализации гибридной угрозы национальной безопасности в высокотехнологической среде предлагается рассмотреть атаку Соединенных Штатов и их союзников на китайскую компанию Huawei, которая иллюстрирует методы борьбы в политико-экономическом конфликте. Как показывает анализ ситуации, главная задача конкурентов КНР заключается в создании непреодолимых препятствий для развития Китаем своего высокотехнологического сектора.

Так, задержание в декабре 2018-го года в Ванкувере по запросу США канадскими властями директора китайской компании Huawei Technologies Мэн Ваньчжоу финансового первоначально мотивировалось нарушениями этой кампанией американских санкций против Ирана. Однако, практически сразу стало ясно, что это формальный предлог, и действительные мотивы этого задержания кроются совершенно в другой плоскости. Поскольку задолго до задержания Мэн Вэньчжоу американские власти, в первую очередь — так называемое «deep state» США, представляющее собой неформальное объединение бизнеса, политиков и разведывательных служб, оказывали давление на своих иностранных партнеров с целью принуждения их к отказу от сотрудничества с Китаем в высокотехнологических секторах. В частности — к отказу от использования телекоммуникационного оборудования, произведенного китайским концерном Huawei.

Для более полного понимания ситуации необходимо отметить, что Huawei играет громадную роль в стратегии «Сделано в Китае 2025» в качестве проводника технологии 5G. Более того, в 2017 году, по данным Всемирной организацией интеллектуальной собственности, Huawei с большим отрывом возглавила список компаний, подавших заявки на международные патенты. А в 2018 году Huawei была названа крупнейшим в мире поставщиком телекоммуникационного оборудования и заняла второе место по количеству производимых смартфонов. Она также обогнала шведскую «Эриксон» и финскую «Нокиа» по количеству коммуникационных станций, выйдя на первое место в мире.

Таким образом, выбор именно этой компании в качестве мишени был наиболее оптимален для администрации Трампа и ее союзников при решении задачи замедления или же, в оптимальном варианте, прекращения продвижения Китая в высокотехнологичных секторах. Особенно — с учетом того, насколько эта компания продвинулась в продвижении технологий 5G.

Кроме того, для реализации этой задачи был избран метод вытеснения китайской компании из мировой (как минимум, западной) экономики нерыночными средствами. То есть — с использованием административно-политического ресурса и возможностей разведывательного сообщества США и его союзников — так называемой полуофициальной структуры «Пять глаз», в которую входят спецслужбы Австралии, США, Канады, Новой Зеландии и Великобритании, а также тесно сотрудничающие с ней спецслужбы Японии и Германии.

Именно эти страны после развития «дела Huawei» практически одновременно приняли меры для запрета или же серьезного ограничения использования оборудования китайской компании при создании сетей 5G, мотивировав свои действия «соображениями национальной безопасности».

Необходимо отметить, что Пекин практически сразу после задержания в Канаде Мэн Ваньчжоу дал предельно адекватную оценку происходящему и не испытывает никаких иллюзий в отношении истинных мотивов действий США и их партнеров.

Кроме того, руководство КНР полностью осознает возникающую для него угрозу этого нового типа конфликта, а потому его ответ носил достаточно жесткий характер. Буквально за неделю с момента задержания Мэн Ваньчжоу в Китае, в качестве ответной меры были задержаны 13 канадских граждан (после освобождения Мэн под залог 8 из них были отпущены и беспрепятственно покинули КНР).

Помимо этого, дипломатические представители Китая по официальным и неофициальным каналам довели до руководства участвовавших в «деле Huawei» государств (в частности — Канады, Японии, Германии и Австралии) информацию о том, что дальнейшие действия против китайской компании повлекут за собой ответные шаги Пекина в торгово-экономических и финансовых отношениях с этими странами.

Вместе с тем, руководство КНР вновь обратило внимание на уязвимость своей высокотехнологической отрасли в следующем вопросе — зависимость от поставок чипов и других комплектующих, которые китайские компании вынуждены закупать в США и ряде других стран на сумму не менее 200 миллиардов долларов ежегодно.

В настоящее время по данному вопросу готовится соответствующее постановление директивных органов КНР, предусматривающее развитие соответствующих

секторов китайской промышленности и выделение для этой задачи необходимого финансирования.

Важно подчеркнуть, что одной особенностью гибридных противостояний является их нелинейный, неравномерный характер. Несмотря на снижение интенсивности процесса на текущий момент, ни в КНР, ни в США «дело Huawei» не считаю законченным. Специалисты этих государств в настоящее время проводят тщательный анализ ситуации, разрабатывая методики для более эффективного использования подобных ситуаций в собственных целях.

В этой связи нельзя не отметить справедливость опасений экспертов, указывающих на то, что обеспечением цифровизации государственного управления в России активно занимаются транснациональные гиганты, представляющие исключительно передовые страны Запада.

Анализ конфликта позволяет констатировать синтез новых средств противоборства с классическими в условиях нарастающей конкуренции на всех уровнях. Странами применяется комплекс мер, включающих в себя нерыночные средства, для создания условий недопущения некоторых объективных политико-экономических трансформаций на глобальном и региональном уровне.

Развитие аналитики безопасности должно быть тесно связано с изучением угроз как разновекторных, комплексных явлений. Методология и теория национальной безопасности находится на стыке наук, интегрируя многообразие подходов и методов междисциплинарного знания.

ЛИТЕРАТУРА

1. Правиков Д.И., Щербаков А. Ю. Изменение парадигмы информационной безопасности // Системы высокой доступности, 2018. № 2. С. 34–39.
2. Гриняев С. Н. Мир 2013: события, факты, комментарии. М.: ЦСОиП, 2014. 328 с.
3. Гриняев С.Н., Правиков Д. И. Основы общей теории киберпространства. Теория боя в киберпространстве. М.: АНО ЦСОиП, 2018. 124 с.
4. Гриняев С.Н., Правиков Д. И. Об одном подходе к описанию сложных социотехнических систем // Информационные войны, 2018. № 2 (46). С. 34–37.
5. Гриняев С.Н., Калашников П. К., Орлов А. И., Самарин И. В., Фомин А. Н., Юнкин А. Г. Научно-методический аппарат антикризисного стратегического планирования М.: РГУ нефти и газа имени И. М. Губкина, 2015. 420 с.
6. Медведев Д.А, Тарчокова А. А. Инструменты международной легитимации внешнеполитических действий России в условиях информационного противоборства // Информационные войны, 2018. № 3. С. 34–37.
7. Самарин И. В., Фомин А. Н. Стратегическое государственное планирование: автоматизация процесса оценки рациональных уровней финансирования национальной обороны // Современная наука: актуальные проблемы теории и практики. Серия «Естественные и технические науки», -2018, — № 6, -С. 136–144