УДК 51-77
DOI: 10.24044/sph.2017.2.6

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ПОТЕНЦИАЛЬНО ОПАСНЫХ ТЕХНОЛОГИЙ В СОВРЕМЕННОМ МИРЕ

О. В. Тиханычев — *Кандидат технических наук, профессор г. Москва, Россия*

Е. О. Тиханычева — *студентка Финансовый университет при Правительстве РФ, филиал, г. Краснодар, Россия*

PROBLEMS OF THE USE OF DANGEROUS TECHNOLOGIES IN THE MODERN WORLD

O. V. Tikhanychev — *Candidate of Technical Sciences, professor Moscow, Russia*

E. O. Tikhanycheva — *student Financial University under the Government of the Russian Federation, filial, Krasnodar, Russia*

Abstract. Our society cannot be imagined without modern technology. But the distribution of these technologies around the world is uneven: somewhere they are developed and somewhere only used. And, as practice shows, technologies are not always used for their intended purpose. Very often, modern information technology is used to the detriment of the developer, for conducting military and terrorist activities. It is difficult to counteract this, but it is possible. The first stage of counteraction should be the recognition of the existence of the problem itself and the need for its solution. After recognizing the need to solve the problem, it is necessary to develop technologies for its solution. The article proposes a number of technological measures that can provide a solution to this problem. The proposed measures may be unpopular and require rigidity in implementation. But their implementation will significantly reduce the opportunities to destabilize modern society.

Keywords: information confrontation; modern technologies; information technology; technology implementation model; illegal use; restriction of use.

Трудно представить существование нашего общества без современных технологий. Но территориально, ареалы распространения этих технологий неравномерны: где-то их разрабатывают и реализуют, а где-то только используют. Причём, как показывает практика, используют разнообразно, но не всегда по прямому назначению.

Примером могут служить информационные технологии, которые в последнее время активно применяются в межгосударственном противоборстве в рамках так называемой «мягкой силы». Активно используются социальные сети при организации разного рода протестных движений. Но, во вред интересам общества, могут использоваться и другие технологии, казалось бы, сугубо утилитарного назначения.

Наглядный пример подтверждения этого тезиса – информационно-коммуникационные технологии коммерческого назначения. В современном мире, оперативная и надёжная связь имеет существенное значение, как в повседневной жизни, так и при реализации всех видов противоборства [1]. Как показала практика, в ходе вооруженных конфликтов различной природы, при организации террористических акций, для организации системы связи часто применяются коммерческие средства и системы двойного

назначения: средства радиосвязи, мобильные телефоны, узловые станции, программное обеспечение. При операциях террористического характера на Ближнем востоке и акциях в Европе – это средства мобильной связи, которые заимствуются у сторонних производителей, беспилотники для ведения разведки и даже нанесения ударов. Реализуются и «нестандартные» подходы: применение мобильных телефонов в качестве дистанционных взрывателей, компьютерных планшетов в качестве баллистических станций управления миномётным огнём и т. п. Организации радикального толка в Европе активно используют для информационного противоборства, кроме социальных сетей, средства управления на основе Интернета и мобильных обменников сообщениями, в том числе программно шифруемые. В последние годы, и, казалось бы, рядовые технические устройства, такие как автомобили, самолёты, беспилотные устройства, тоже используются как оружие.

Конечно, средства «мирного» назначения – не основное оружие в современном противоборстве. Организации террористической направленности активно используют обычное оружие и боеприпасы, технологиями производства которых, кстати, тоже не владеют. Но, как показывает опыт, эффективно вести согласованные действия на больших территориях, даже имея достаточно оружия, без средств коммуникации, невозможно [2]. И информация и коммуникации в современных операциях часто важнее, чем оружие.

В итоге складывается парадоксальная ситуация: технологии наиболее активно используются во вред обществу там, где их вообще не разрабатывают. Часто случается, что используются против самих разработчиков. Противостоять этому пока не удаётся, в первую очередь потому, что проблема не акцентирована. Для начала нужно её хотя бы обозначить, и тогда уже искать эффективные пути решения.

Именно из-за сложившейся модели использования новых технологий, в современных условиях тезис военных теоретиков XX века о том, что бороться с незаконными вооруженными формированиями нужно, переводя военные действия в недоступную им высокотехнологичную сферу [3, 4, 5], не работает. Не работает, так как многие используемые в террористических актах и «гибридных» войнах технологии, как отмечалось ранее – это высокотехнологичные средства коммерческого и двойного назначения [6, 7, 8]. И доступ к ним сейчас может получить каждый, кто в состоянии заплатить.

Для эффективного противодействия сложившейся ситуации нужно в первую очередь признать, что существующая модель создания и использования технологий, в том числе информационных – неэффективна с точки зрения безопасности общества. Впрочем, это уже начинают понимать, даже «политкорректных» в США и Европе [9]. Может быть, это прозвучит не демократично, но для обеспечения безопасной модели применения технологий, вероятно, стоит отказаться при их разработке и организации эксплуатации от ряда базовых принципов. Речь идёт даже не о контроле информационного трафика, который реализуется уже сейчас, например, в Китае. Во-первых, как показала практика, эта мера недостаточно эффективна, её можно обойти. Во-вторых, контроль трафика не решает проблемы использования во вред людям утилитарных технических средств.

В рамках создания новой модели, вероятно, потребуется отказаться от реализуемого сейчас в информационной отрасли принципа «разрешено всё, что не запрещено», в пользу менее демократичного, но существенно более безопасного «запрещено всё, что не разрешено». С точки зрения технологий это:

- разрешение доступа к технологически и социально опасным программным средствам и сегментам коммуникацион-

ных сетей только при наличии соответствующих прав;

- обязательная авторизация при входе в любую коммуникационную сеть с заданием прав доступа пользователям;

- обеспечение возможности отключения отдельных сегментов коммуникационных сетей по самым разным признакам: территориальным, по уровню допуска и т. п.;

- и, в дополнение, непрерывный мониторинг коммуникационных сетей с целью поиска угроз безопасности.

С технологической точки зрения все эти меры сложны, но реализуемы. Сами возможности их реализации заложены в самих современных технологиях:

- подавляющее большинство современных коммуникационных устройств обеспечивают возможность идентификации пользователя, не только по ключу, но с использованием статических и динамических биометрических признаков, в том числе независимо от его желания. Это позволит не только собирать статистику для прогнозирования угроз, но и обеспечивать временное ограничение прав доступа (в том числе автоматически) и поиск местонахождения отдельных пользователей;

- развитие «интернета вещей» (Internet of Things, IoT), в первую очередь промышленного (Industrial Internet of Things, IIoT), обеспечит дистанционный контроль над техногенно-опасными системами, в перспективе, за счёт внедрения специализированных алгоритмов – существенно затруднит использование в качестве орудия терактов транспортных и других технических средств повышенной опасности.

Можно привести множество подобных примеров. Часть таких возможностей уже реализуется, хоть и с существенными ограничениями [10, 11, 12]. Проблема не в технологии реализации указанных мер, а в этической сфере: в интересах безопасности потребуется пожертвовать рядом экономических и социальных свобод. Но жертва части личных «свобод» ради общественной безопасности – это вполне логичный шаг. Он намного гуманнее постепенно складывающейся нестабильной ситуации, ведущей к саморазрушению человеческого общества, в том числе, из-за нецелевого использования современных технологий.

Библиографический список

1. Выпасняк В. И. и др. Кибер-угрозы автоматизированным системам управления // Вестник Академии военных наук. – 2013. – № 1 (42). – С. 103–109.
2. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ № 646 от 5 декабря 2016 г.).
3. Домнин И. В. От Первой мировой до «Третьей Всемирной». Жизненный путь Генерального штаба полковника Е. Э. Месснера / Хочешь мира, победи мятежевойну! Творческое наследие Е. Э. Месснера / Ответственный за выпуск И. В. Домнин. – М.: Военный университет, Русский путь, 2005. – Т. 21. – С. 18–51. – 696 с.
4. Домнин И. В., Савинкин А. Е. Асимметричное воевание // Отечественные записки: журнал. – 2005. – № 5.
5. Месснер Е. Всемирная мятежевойна. – М. : Кучково поле, 2004 – 512 с.
6. О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статью 14 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». 188-ФЗ от 29.07.2015 года.
7. Тиханычев О. В. Об учёте межгосударственных границ при моделировании межэтнического взаимодействия // Социосфера. – 2014. – № 2. – С. 197–201.
8. Тиханычев О. В., Тиханычева Е. О. Некоторые аспекты моделирования этносоциальных процессов. – М. : Эдитус, 2016. – 70 с.
9. Шишло А. Близкие погибших при терактах в Брюсселе и Париже подали иск против Twitter. Новости Mail.Ru. 10.01.2017. URL: https://news.mail.ru/society/28380584/?frommail=1.
10. Стратегия развития информационного общества в Российской Федерации на период 2017–2030 годы. Утверждена Указом Президента Российской Федерации от 9.05.2017 № 203.
11. Манойло А. В. Модели «мягкой силы» сетевых террористических организаций (на примере Исламского государства, Аль-Кайды, Талибана и Братьев мусульман) // Геополитический журнал. 2016. – № 2 (14). – С. 37–46.

12. UK Prime Minister Theresa May Blames Internet for Terrorism, Internet Bites Back. URL: https://sputniknews.com/europe/201706051054329173-uk-terror-encryption-may.

Bibliograficheskij spisok

1. Vypasnjak V. I. i dr. Kiber-ugrozy avtomatizirovannym sistemam upravlenija // Vestnik Akademii voennyh nauk. – 2013. – № 1 (42). – S. 103–109.
2. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii (utverzhdena Ukazom Prezidenta RF № 646 ot 5 dekabrja 2016 g.).
3. Domnin I. V. Ot Pervoj mirovoj do «Tret'ej Vsemirnoj». Zhiznennyj put' General'nogo shtaba polkovnika E. Je. Messnera / Hochesh' mira, pobedi mjatezhevojnu! Tvorcheskoe nasledie E. Je. Messnera / Otvetstvennyj za vypusk I. V. Domnin. – M.: Voennyj universitet, Russkij put', 2005. – T. 21. – S. 18–51. – 696 s.
4. Domnin I. V., Savinkin A. E. Asimmetrichnoe voevanie // Oteche-stvennye zapiski: zhurnal. – 2005. – № 5.
5. Messner E. Vsemirnaja mjatezhevojna. – M. : Kuchkovo pole, 2004 – 512 s.
6. O vnesenii izmenenij v Federal'nyj zakon «Ob informacii, informacionnyh tehnologijah i o zashhite informacii» i stat'ju 14 Federal'nogo zakona «O kontraktnoj sisteme v sfere zakupok tovarov, rabot, uslug dlja obespechenija gosudarstvennyh i municipal'nyh nuzhd». 188-FZ ot 29.07.2015 goda.
7. Tihanychev O. V. Ob uchjote mezhgosudarstvennyh granic pri modelirovanii mezhjetnicheskogo vzaimodejstvija // Sociosfera. – 2014. – № 2. – S. 197–201.
8. Tihanychev O. V., Tihanycheva E. O. Nekotorye aspekty modelirovanija jetnosocial'nyh processov. – M. : Jeditus, 2016. – 70 s.
9. Shishlo A. Blizkie pogibshih pri teraktah v Brjussele i Parizhe podali isk protiv Twitter. Novosti Mail.Ru. 10.01.2017. URL: https://news.mail.ru/society/28380584/?frommail=1.
10. Strategija razvitija informacionnogo obshhestva v Rossijskoj Federacii na period 2017–2030 gody. Utverzhdena Ukazom Prezidenta Rossijskoj Federacii ot 9.05.2017 № 203.
11. Manojlo A. V. Modeli «mjagkoj sily» setevyh terroristicheskih organizacij (na primere Islamskogo gosudarstva, Al'-Kajdy, Talibana i Brat'ev musul'man) // Geopoliticheskij zhurnal. 2016. – № 2 (14). – S. 37–46.
12. UK Prime Minister Theresa May Blames Internet for Terrorism, Internet Bites Back. URL: https://sputniknews.com/europe/201706051054329173-uk-terror-encryption-may.