References

1. Abalkin A. Jekonomicheskaja bezopasnost' Rossii: ugrozy i ih otrazhenie // Voprosy jekonomiki. 1994. № 12. S. 4–13.
2. Senchagov V. Jekonomicheskaja bezopasnost' Rossii // JeKO. 2007. № 5. S. 2–20.
3. Vechkanov G. Jekonomicheskaja bezopasnost'. SPb.: Vektor, 2005. 384 s.
4. Aleksej Nevel'skij. Neravenstvo meshaet rostu // Vedomosti. 2014. 10 dekabrja.
5. Rossijskaja gazeta. 2014. 28 maja.
6. Konstantin Gurdin. Kreml' bankrotit regiony // Argumenty nedeli. № 19. 28 maja-3 ijunja. 2015.
7. Evgenija Pis'mennaja. Uravnjat' za trillion // Vedomosti. 2013. 25 janvarja.
8. Mihail Deljagin. Rossija. Krizis. Tretij srok… // Zavtra. Nojabr'. 2011. № 46.
9. Shamil' Sultanov. Zabytaja tajna Sovetskogo Sojuza // Zavtra. Sentjabr'. 2010. № 37.
10. Rossijskaja Federacija segodnja. Dekabr'. 2003. № 24.
11. Rossijskaja gazeta. 2006. 7 nojabrja.
12. Argumenty i fakty, № 44, 2014 g.
13. Izvestija. 2011. 14 aprelja.
14. Sovetskaja Rossija. 2014. 1marta.
15. Viktor Trushkov. Tretij orden dadut ili vse zhe otpravljaet v tjur'mu? // Pravda. 2015. 12 marta.
16. Valerij Zor'kin. Konstitucija protiv kriminala // Rossijskaja gazeta. 2010. 10 dekabrja.

УДК 32

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ НЕТРАДИЦИОННЫМ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Курников Ефим Васильевич кандидат экономических наук,
доцент кафедры международных экономических отношений,
Южно-Российский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте РФ (344002, Россия, г. Ростов-на-Дону, ул. Пушкинская, 70/54).
E-mail: kurnikov.efim@gmail.com

Аннотация

Информационная безопасность постоянно сталкивается с новыми вызовами из-за широкого распространения устройств для получения несанкционированного доступа к информации, а именно разведывательных беспилотных летательных аппаратов. В статье рассматриваются основные проблемы противодействия этой угрозе и мероприятия, необходимые для ее уменьшения.

Ключевые слова: *беспилотный летательный аппарат, БПЛА, информационная безопасность, разведка*.

В современных условиях одной из определяющих тенденций глобального социально-экономического развития является широкомасштабное применение цифровых и информационных технологий во всех сферах человеческой деятельности. С одной стороны, этот процесс оказывает благотворное влияние и позволяет намного более эффективно использовать имеющиеся у человечества ресурсы и возможности. С другой стороны, взрывной рост использования цифровых технологий передачи и обработки информации порождает значительное количество критических уязвимостей и «слепых пятен» в активно формирующейся инфраструктуре информационного общества XXI века.

Кроме того, внедрение информационно-коммуникационных технологий приводит к перераспределению возможностей воздействия на окружающий мир как между привычными участниками процессов государственного и корпоративного управления, так и между новыми претендентами на получение властных полномочий, гласных или негласных. Отсутствие необходимости физического доступа

к различным объектам социально-экономической и культурно-коммуникационной инфраструктуры, а также новые возможности по манипулированию и прямому (в некоторых случаях несанкционированному) управлению ими приводят к формированию новых групп лиц, заинтересованных в перераспределении активов и власти в свою пользу.

Важнейшей особенностью происходящих процессов является постепенный переход от производственно-финансового к информационно-аналитическому характеру экономики, что обуславливает использование информации и возможностей ее анализа и интерпретации как основного фактора производства. Хотя такая трансформация экономической действительности не предполагает отмирания классических производственных отношений, ее очевидным следствием становится концентрация основных усилий общества и бизнеса вокруг рынка информации и информационных услуг. Таким образом, информация выступает новым, в какой-то степени универсальным, эквивалентом ценности всего, в том числе и материальных активов.

Исходя из этого, значительные усилия уже сейчас направляются на сбор и анализ общедоступной информации, а также на получение служебной, личной, секретной информации любыми возможными способами. Особую значимость такая деятельность приобретает в связи с поэтапным внедрением новых принципов обработки «Big Data», массивов данных, собираемых глобально в автоматическом режиме. С течением времени и появлением еще более совершенных технологий подобные процессы только ускорятся.

Общество и государство далеко не всегда успевают адаптироваться к нарастающим изменениям и разработать сбалансированную реакцию, в том числе меры противодействия вновь возникающим угрозам. Частично это связано с общей инерцией государственного аппарата и длительными сроками, необходимыми для изменения законодательства, но в немалой степени замедленная реакция на угрозы связана с их внешне незначительным характером и малой известностью, а также с надеждой на срабатывание уже существующих, опробованных механизмов.

Так, до последнего времени не получила должного внимания весьма значимая проблема, связанная с обеспечением информационной безопасности в случае применения нетрадиционных средств для несанкционированного доступа к информации. По данным журнала Spiegel, государственные органы власти Соединенных Штатов Америки разработали и применяют комплекс аппаратно-программных средств для получения различных видов защищаемой информации бесконтактным путем и добились в этом значительных результатов.

Он функционирует в рамках системы операций адресного доступа (Tailored Access Operations), которые являются одним из важнейших направлений деятельности Агентства национальной безопасности (АНБ) США и выполняются соответствующим подразделением. Его основная задача состоит в получении доступа к информационно-коммуникационным сетям и устройствам по всему миру, вне зависимости от уровня их защищенности и включенности в глобальные телекоммуникационные сети. Для этого используются программно-аппаратные комплексы, объединенные под общим наименованием QUANTUM. Существует также достаточно большое количество специализированных систем, выступающих под такими несколько ироничными наименованиями, как NIGHTSTAND, IRONCHEF, COTTONMOUTH-II, CTX4000, NIGHTWATCH, WATERWITCH и другими.

Особо необходимо отметить системы и устройства, позволяющие получать информацию с компьютеров, не подключенных к коммуникационным сетям. Это приемо-передающий радарный комплекс CTX4000/PHOTOANGLO и устройство обработки и отображения NIGHTWATCH или его аналоги. Кроме того, в систему входят и передающие устройства, по возможности размещающиеся на объектах, доступ к которым требуется получить, такие как VIEWPLATE, VAGRANT, LOUDAUTO, DROPMIRE, RAGEMASTER, SURLYSPAWN и другие [1].

Такие действия специальных служб различных государств являются достаточно распространенной и в какой-то степени привычной угрозой, методы противодействия которой известны и используются компетентными органами. К сожалению, практически незамеченной осталась проблема личного и коммерческого использования аналогичных технологий.

Так, наличие и широкое распространение БПЛА позволяет в короткие сроки создать малозаметное средство шпионажа, не отличающееся высокой сложностью или стоимостью изготовления. При этом необходимо учитывать, что потенциальный ущерб от применения подобных средств значительно выше хотя бы за счет в разы более масштабного охвата потенциальных жертв и значительно большего объема чувствительной информации, в том числе финансовой и медицинской.

В отличие от традиционных методов сбора закрытой информации БПЛА предоставляют значительно больший спектр возможностей, что в первую очередь связано с их техническими характеристиками. Существует и активно используется достаточно широкая номенклатура беспилотников, которые зачастую относятся к одному из двух типов:

- самолетному (классическая схема с несущими крыльями и тянущим либо толкающим винтом);
- вертолетному (классический одновинтовой вертолет и различные многовинтовые конструкции, такие как квадрокоптеры).

Имеются также проекты и отдельные модели БПЛА, использующие иные принципы создания подъемной силы и перемещения, в том числе до определенных пределов имитирующие способ полета птиц и насекомых, например орнитоптеры.

Размеры и грузоподъемность могут значительно варьироваться в зависимости от предполагаемых функций аппарата. Применяются различные классификации БПЛА по этим признакам, в частности американская военная, но всех их можно систематизировать следующим образом:

- микро БПЛА (взлетная масса до 1 кг);
- мини БПЛА (взлетная масса до 50 кг);
- средние БПЛА (взлетная масса до 1000 кг);
- тяжелые БПЛА (взлетная масса свыше 1000 кг).

Необходимо также выделить основные формы функционирования БПЛА:

- дистанционно пилотируемый летательный аппарат (непрерывное управление всеми функциями и устройствами осуществляется с пункта управления на земле);
- беспилотный автоматический летательный аппарат (работает в автоматическом режиме в соответствии с заложенными в его систему управления алгоритмом и программами функционирования);
- дистанционно управляемый летательный аппарат (непрерывное управление осуществляется тем или иным способом с пункта управления, но оператор концентрируется на необходимом результате работы, а за непосредственное пилотирование отвечает автоматика);
- дистанционно управляемая авиационная система (работает за счет выполнения внутренних динамических алгоритмов при эпизодическом вмешательстве оператора, функции которого сводятся к управлению задачами групп БПЛА и контролю их поведения).

Варианты применения робототехники, в частности беспилотных летательных аппаратов, на данный момент весьма обширны. В этой связи значительный интерес представляют темпы внедрения БПЛА в деятельность коммерческих организаций, формально не связанных с нелегальным доступом к информации. Особого внимания заслуживает работа компаний, подобных сингапурской AdNear, которая стала применять квадрокоптеры именно для этих целей. В феврале 2015 г. она запустила некоторое количество БПЛА в Лос-Анджелесе с целью отслеживать и перехватывать содержимое передач Wi-Fi и сотовой связи. Официально заявлено, что собираются обезличенные данные об устройствах, передаваемой информации, местоположении и предпочтительных маршрутах передвижения. Компания не собирает личные данные граждан и не хранит перехваченные разговоры, номера телефонов и файлы сети Интернет. Тем не менее, такие действия вызывают серьезную озабоченность, так как компания различными способами накопила данные на 530 млн устройств и их пользователей из различных стран и не собирается останавливаться на этом [2].

Не менее важно и широкое распространение самодельных устройств для получения несанкционированного доступа к информации на базе различных БПЛА и комплектующих, находящихся в свободной продаже. Так, активно распространяется проект беспроводной платформы воздушной разведки (Wireless Aerial Surveillance Platform), построенный именно из таких элементов. Эта платформа позволяет перехватывать сигнал Wi-Fi и сотовой связи с целью прослушивания разговоров, чтения

SMS-сообщений, просмотра информации из сети Интернет. За счет модульной конструкции возможно ее переоснащение под другие цели, в том числе перехват видео- и аудиосигналов [3].

Появление подобных БПЛА приобретает еще более угрожающий характер в связи с возможностью их использования в дистанционных атаках на компьютеры и сети, даже не подключенные к Интернет. Необходимое для этого оборудование, применяемое АНБ в рамках системы TEMPEST, уже не является насущной необходимостью в связи с разработками исследователей Университета Бен-Гуриона (Израиль). Они сумели добиться дистанционного заражения мобильного телефона вирусом с его последующей трансформацией в станцию слежения за электромагнитным излучением компьютеров с целью получения доступа к хранящимся на них данным [4].

Традиционные способы противодействия таким атакам малопригодны к использованию, так как зачастую базируются на применении средств радиоэлектронной борьбы или зенитного вооружения, что невозможно в условиях мирного времени. Необходимо приложить значительные усилия для разработки адекватного ответа на эту и подобные ей угрозы информационной безопасности. Речь может идти как о разработке нормативно-правовой базы, регламентирующей функционирование БПЛА, так и о проведении специальных мероприятий по выявлению и предупреждению актов несанкционированного доступа к информации. В любом случае необходима скоординированная деятельность компетентных органов для минимизации негативных последствий этих угроз.

Литература

1. http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-1.html
2. http://thehackernews.com/2015/03/drone-cell-phone-spy.html
3. http://securityaffairs.co/wordpress/31190/hacking/wireless-aerial-surveillance-platform-diy-spy-drone.html
4. http://securityaffairs.co/wordpress/25782/hacking/air-gap-network-hacking.html

***Kurnikov Efim Vasilyevich*,** PhD Economics, Associate Professor of International economic relations chair; South-Russia Institute of Management – branch of Russian Presidential Academy of National Economy and Public Administration (70/54, Pushkinskaya St., Rostov-on-Don, 344002, Russian Federation).
E-mail: kurnikov.efim@gmail.com

PROBLEMS OF COUNTERING UNCONVENTIONAL THREATS TO INFORMATION SECURITY

Abstract

Information security is constantly facing new challenges in no small part due to readily available devices for gaining unauthorized access to information, namely intelligence drones. The article discusses major problems of addressing this threat and measures necessary for its mitigation.

Keywords: *drone, unmanned aerial vehicle, information security, intelligence.*

References

1. http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-1.html
2. http://thehackernews.com/2015/03/drone-cell-phone-spy.html
3. http://securityaffairs.co/wordpress/31190/hacking/wireless-aerial-surveillance-platform-diy-spy-drone.html
4. http://securityaffairs.co/wordpress/25782/hacking/air-gap-network-hacking.html