УДК 34.096

Галушкин А.А.
Международный институт информатизации и государственного управления им. П.А. Столыпина, г. Москва

КИБЕРШПИОНАЖ – УГРОЗА СОВРЕМЕННОМУ ИНФОРМАЦИОННОМУ ОБЩЕСТВУ*

Аннотация. В статье рассмотрена одна из наиболее актуальных проблем современного информационного общества – кибершпионаж. Приведены результаты анализа различных аспектов кибершпионажа, и на его основе выдвинуты организационно-правовые предложения по противодействию ему исследуемому виду правонарушений. По мнению автора, последнее может способствовать обеспечению режима законности и правопорядка. В частности, отмечается целесообразность создания специализированной службы, способной отвечать меняющимся вызовам современного информационного общества, наделенной необходимыми кадровыми и материально-техническими ресурсами для оперативной компетентной реализации своих узкоспециализированных полномочий в рамках специальной подследственности.
Ключевые слова: информационная безопасность, информационное общество, компьютерная преступность, кибершпионаж.

A. Galushkin
International Institute of Informatization and Public Administration Named after P.A. Stolypin, Moscow

CYBERESPIONAGE – THREAT TO MODERN INFORMATION SOCIETY

Abstract. The article deals with one of the most acute problems of modern information society – the problem of cyberespionage. The author analyzes various aspects of cyberespionage and makes some organizational and legal propositions to counteract cyberespionage. One of them is the creation of a special service capable of meeting the challenges of modern information society and possessing necessary labour resources and technical facilities to implement its tasks within special jurisdiction.
Key words: information security, information society, cybercrime, cyberespionage.

«Каждое из направлений развития информационного общества, – справедливо отмечает профессор И.Л. Бачило, – касается реализации прав и интересов человека и ответственности субъектов, нарушающих установленный порядок противоправными действиями и бездействиями, а также деятельности правоохранительных и судебных органов в области защиты прав человека и гражданина в пределах, реализующих их компетенцию и правовой статус» [2, с. 169]. На протя-

* Работа выполнена при финансовой поддержке гранта Президента РФ № МК-4283.2015.6.

жении многих лет в Российской Федерации, как и во многих странах мира, по мнению автора, на государственном уровне не уделялось достаточного внимания вопросам правового регулирования порядка использования информационных технологий. В силу этого за противоправные действия фактически отсутствовала ответственность.

Еще меньше внимания уделялось вопросам профилактики правонарушений, предотвращения преступлений и их расследования. Если говорить о правовом регулировании деятельности в российском сегменте глобальной информационно-телекоммуникационной сети «Интернет» (далее – РуНЕТ), то за многие годы слабого правового режима возникла среда с очень низкой правовой культурой и многими проявлениями режима беззакония. «Излишне говорить, какое значение для поддержания правопорядка в рамках государства и в межгосударственных отношениях имеет единообразие понимания толерантности, уважения личности и имиджа государства, обеспечения правовой защиты религиозной, этнической культуры многонационального социума планеты» [5, с. 45].

С развитием информационных технологий стали разрабатываться инструменты для шпионажа с использованием как специализированных устройств, так и программного обеспечения. В отличие от классических методов разведки и шпионажа, новые технологии внесли в них существенные корректировки. В настоящее время иногда невозможно установить, кто именно разработал то или иное программное обеспечение для проведения разведывательных действий в сфере высоких технологий (кибершпионажа). Разработчиками подобного специализированного программного обеспечения являются и частные лица, и организации различной организационно-правовой формы, с различными источниками финансирования (в том числе, в отдельных случаях, и с государственным участием). Часто лица, разработавшие программное обеспечение или специальное оборудование, не являются теми же лицами, которые его используют для осуществления кибершпионажа. Это затрудняет, а иногда делает невозможным, идентификацию лиц, осуществляющих кибершпионаж, и как результат – их привлечение к установленной форме ответственности. Подобная практика приводит к тому, что заинтересованные лица чаще всего самостоятельно изыскивают методы противодействия проявлениям кибершпионажа в каждом конкретном случае. Последние включают в себя классические методы повышения информационной защищенности объектов, а также специализированные методы кибер-контрразведки.

В отличие от встречающегося мнения, что объектами нападения в кибершпионаже являются международные, межгосударственные, государственные органы, организации и учреждения, на деле объектами часто оказываются коммерческие компании и предприятия. Однако, по каким-то причинам этому обстоятельству не уделялось должного внимания, особенно если это не было связано с хищением государственной тайны. Кибершпионы нередко ставят целью кражу массива информации, поскольку такие действия позволяют получать большое количество персональных данных и/или коммерчески значимой

информации. Целью может также быть изменение или удаление определенной информации, что позволяет устранить компрометирующие сведения, создать положительную (отрицательную) историю или, к примеру, создать определенные условия для совершения другого противоправного действия.

Кибершпионы стремятся похитить финансовую информацию в «условиях глобализации, когда информационные финансовые отношения не знают территориальных границ, а международных соглашений о пределах юрисдикций государств все еще нет» [7, с. 236]. Целью хищения нередко становятся не сами денежные средства, а информация (к примеру, не опубликованный годовой отчет), которая может позволить, к примеру, «сыграть» на акциях компании. Принимая во внимание, что благоприятное состояние информационной жизни общества является «условием, без которого невозможно ожидать социально-полезного результата от идеи и процессов формирования информационного общества» [3, с. 32], а также тот факт, что «в качестве новых угроз экономической безопасности в условиях информационной экономики» все чаще рассматривается «кибершпионаж» [9, с. 28], необходимо создание адекватного комплекса механизмов по своевременному выявлению киберугроз.

Необходимо понимать, что сама киберугроза «может быть как неумышленной, так и намеренной, нацеленной или не нацеленной, она может исходить из множества различных источников, включая иностранные государства, осуществляющие шпионскую деятельность и информационные войны, преступников, хакеров, создателей вирусов, определенных сотрудников и подрядчиков, работающих в организации» [11, с. 119]. В зависимости от указанных особенностей необходимы различные подходы. С нашей точки зрения, наибольшую опасность представляет преднамеренный, осознанный кибершпионаж. «Мотивами для этих нападений, по-видимому, являются возможности совершения кражи и совершения акта промышленного шпионажа против стран и коммерческих конкурентов. Нападение на компании и организации в финансовом и даже политическом секторе позволяет получить доступ к ценным разведданным в этих областях» [14, с. 50].

Работа по пресечению намеренных противоправных действий видится невозможной без четкого понимания наиболее значимых политических факторов развития компьютерной преступности. К «числу наиболее значимых политических факторов, определяющих развитие компьютерной преступности в Российской Федерации, следует отнести: 1) развитие хактивистского движения как политического протестного движения против государственного контроля в глобальной информационной сети «Интернет» и против соблюдения государством информационных прав человека; 2) причинение вреда государственным интересам, деятельности механизма государственной власти Российской Федерации вооруженными силами враждебных стран, путем использования вредоносных компьютерных программ в качестве информационного оружия; 3) деятельность спецслужб иностранных государств в отношении российских органов власти, учреждений, предприятий для получе-

ния информации геополитического, военно-технического, дипломатического и иного стратегического характера, т. е. «кибершпионаж»» [6, с. 41]. Особое значение указанные проблемы приобретают для Российской Федерации с учетом фактического отсутствия эффективно функционирующего, закрепленного на законодательном уровне правового механизма обеспечения информационной безопасности, существенного отставания России от большинства развитых государств и ряда государств с переходной экономикой по уровню внедрения информационно-коммуникационных технологий [8, с. 4].

Как отмечают специалисты, «существует много случаев кибершпионажа, которые никогда не будут известны, и все-таки шпионаж существует для того, чтобы никогда не быть выявленным. К счастью, было несколько случаев кибершпионажа, которые были не только обнаружены, но также заявлены, и в некоторых случаях проанализированы» [10, с. 5]. Однако, «существование и развитие любой отрасли права связано с реальным состоянием общества. Это прослеживается на истории классических отраслей права: гражданского, уголовного, административного, конституционного. Правовая система – это живая область позитивного права. Она, будучи регулятором общественных отношений в своей совокупности, сама подвержена влиянию динамики экономических, социальных, политических условий жизни социума» [1, с. 95]. По аксиоме, «информационное общество может быть таковым только при условии, что оно является обществом гражданским, социальным, демократическим и правовым» [4, с. 54].

В силу своей природы кибертерроризм и кибершпионаж «бросают вызов областям исследования частично из-за крупного масштаба действий и событий, имеющих место» [12, с. 42]. Подобная особенность кибершпионажа, на наш взгляд, делает единственно возможным и целесообразным консолидацию усилий по обеспечения национальной информационной безопасности в одной федеральной службе. «Слабые места в информационной безопасности продолжат существовать до тех пор, пока развиваются новые технологии для обхода систем безопасности, однако компании могут внедрить последовательную систему управления информационной безопасностью <...>. Шаги могли бы включать внедрение ряда решений: политики безопасности предприятия, программы осведомленности о безопасности, обучение пользователей в сфере безопасности и средств устрашения» [13, с. 30]. Создание подобной службы позволит организовать единые подходы по обеспечению режима безопасности и правопорядка на национальном уровне, а в случае наличия должной политической воли и международной конъюнктуры – на международном уровне.

В условиях сложной экономической ситуации немаловажными являются консолидация материальных ресурсов и кадрового состава. Это позволит при условии создания должных организационно-правовых механизмов обеспечить необходимый режим национальной информационной безопасности, эффективно использовать бюджетные средства и имеющийся кадровый потенциал, эффективно противодействовать актам кибершпионажа, а также иным угрозам национальной информационной безопасности. По мнению

автора, такая служба должна быть наделена широкими полномочиями в соответствии с российским Кодексом об административных правонарушениях и Уголовным-процессуальным кодексом. Подобный подход позволит создать «живую» структуру, способную отвечать меняющимся вызовам современного информационного общества. Наделенная необходимыми кадровыми и материально-техническими ресурсами для оперативной компетентной реализации своих узкоспециализированных полномочий в рамках специальной подследственности, такая служба положительно повлияет на состояние информационной защищенности, уровне законности и правопорядка в российском сегменте национально информационно-телекоммуникационной сети «Интернет».

ЛИТЕРАТУРА:

1. Бачило И.Л. Исчерпаны ли конституционные основы развития информационного общества и информационного права // Государство и право. 2013. № 12. С. 95–108.
2. Бачило И.Л. Обеспечение безопасности интернет-среды: правовые методы и толерантность отношений против киберпреступности // Право цифровой администрации в России и во Франции: сб. мат. российско-франц. междунар. конф. (г. Москва, 27-28 февр. 2013). М.: Конон-плюс, 2014. С. 168–177.
3. Бачило И.Л. О законодательстве в информационной сфере отношений // Информационное общество. 2001. № 4. С. 25–32.
4. Бачило И.Л. О неизбежном продолжении разговора о публичных услугах и более общих проблемах организации государственного управления (по поводу статьи И.Н. Барцица) // Государство и право. 2014. № 4. С. 53–57.
5. Бачило И.Л. Право и закон: инфокоммуникативный аспект // Труды ин-та государства и права РАН. 2013. № 4. С. 37–47.
6. Евдокимов К.Н. Политические факторы компьютерной преступности в России // Информационное право. 2015. № 1. С. 41–47.
7. Тедеев А.А. Социально-экономическая и интеграционная роль регламентации валютных операций в финансовой политике стран СНГ в условиях развития интернет-технологий // Бизнес в законе: экономико-юридический журнал. 2010. № 3. С. 236–238.
8. Тедеев А.А. Ценностные ориентиры государственной инновационной политики в сфере обеспечения устойчивого развития электронного бизнеса в России // Финансы и кредит. 2012. № 14. С. 2–6.
9. Ческидов М.А. Влияние развития информационной экономики на экономическую безопасность государства // Вестник Саратовского гос. соц.-экон. ун-та. 2013. № 3. С. 28–33.
10. Adkins G. Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism // J. of Strategic Security. 2013. Vol. 6 (№ 3, Suppl.). P. 1–9.
11. Ghari W., Shaabi M. Cyber Threats In Social Networking Websites // International J. of Distributed and Parallel Systems. 2012. Vol. 3 (№ 1). P. 119–126.
12. Luppicini R. Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research // Global Media J. (Canadian Edition). 2014. Vol. 7 (№ 1). P. 35–50.
13. Opala O.J., Rahman S.M. Corporate Role in Protecting Consumers from the Risk of Identity Theft // International J. of Computer Networks & Communications. 2013. Vol. 5 (№ 5). P. 19–33.
14. Siboni G., Y.R. What Lies behind Chinese Cyber Warfare // Military and Strategic Affairs. 2012. Vol. 4 (№ 2). P. 49–64.