К ВОПРОСУ О КИБЕРШПИОНАЖЕ И КИБЕРКОНТРРАЗВЕДКЕ НА СОВРЕМЕННОМ ЭТАПЕ

А.А. Галушкин

Кафедра судебной власти, правоохранительной и правозащитной деятельности
Российский университет дружбы народов
ул. Миклухо-Маклая, 6, Москва, Россия, 117198

В статье автор анализирует угрозу кибершпионажа, вызванную широким распространением информационных технологий, анализирует возможные методы противодействия.

Ключевые слова: кибершпионаж, угрозы, информационная безопасность, национальная безопасность, киберконтрразведка.

За последние несколько десятилетий информационные технологии прочно вошли в повседневную жизнь практически каждого человека и работу большинства юридических лиц. При этом следует отметить, что активное развитие информационных технологий связано в первую очередь не с разработкой нового оборудования, а с созданием более совершенного, функционального и удобного в использовании программного обеспечения.

Существенный толчок развитию технологий дала популяризация и активное использование в различных процессах глобальной информационно-телекоммуникационной сети Интернет. «Сегодня можно говорить, что Интернет охватывает все страны мира, так как с применением новых технологий (использование мобильных спутниковых устройств связи) возможно подключение к сети Интернет с любой точки земного шара. Если же говорить о развернутой инфраструктуре, то в таком контексте Интернет охватывает сегодня более 150 стран мира» [3].

Как справедливо отметила И.Л. Бачило, «каждое из направлений развития информационного общества касается реализации прав и интересов человека и ответственности субъектов, нарушающих установленный порядок противоправными действиями и бездействиями, а также деятельности правоохранительный и судебных органов в области защиты прав человека и гражданина в пределах, реализующих их компетенцию и правовой статус» [2].

Однако, как справедливо отметил В.Ф. Яковлев, «у нас сейчас есть… важные социальные сферы, в которых Право пока еще, к сожалению, слабо представлено. Первая — это Интернет. Интернет — величайшее благо, пока оно не превратилось в величайшее зло…» [5].

На протяжении многих лет, по мнению автора, в Российской Федерации, как и во многих странах мира, на государственном уровне не уделялось достаточного внимания вопросам правового регулирования порядка использования

многих информационных технологий, в силу чего за многие противоправные действия фактически отсутствовала ответственность, а еще меньше внимания уделялось вопросам профилактики правонарушений, предотвращения преступлений и их расследования.

В частности, если говорить о правовом регулировании деятельности в Российском сегменте глобальной информационно-телекоммуникационной сети Интернет за многие годы слабого правового режима возникла среда с очень низкой правовой культурой и во многих проявлениях режимом беззакония.

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 подчас невозможно установить, кто именно разработал то или иное программное обеспечение для проведения разведывательных или шпионских действий в сфере высоких технологий (далее — киберкшионаж). Разработчиками подобного специализированного программного обеспечения являются как частные лица, так и организации различной организационно-правовой формы с различными источниками финансирования (в том числе в отдельных случаях и с государственным участием).

Подчас, лица, разработавшие программное обеспечение или специальное оборудование, не являются теми же лицами, которые его используют в своей шпионской деятельности, что часто приводит к невозможности установить лицо, осуществляющее шпионах и привлечение данного лица к ответственности.

Подобная практика приводит к тому, что заинтересованные лица чаще всего самостоятельно изыскивают методы противодействия проявлениям кибершпионажа в каждом конкретном случае. Подобные методы включают в себя классические методы повышения информационной защищенности объектов, а также специализированные методы киберконтрразведки.

В отличие от общепринятого мнения, когда объектами нападения в кибершпионаже являются коммерческие компании и предприятия, на самом деле объектами также являются и международные, межгосударственные, государственные органы, организации и учреждения, однако по каким-то причинам часто этому не уделялось должного внимания, особенно в случаях, если это не было связано с хищением государственной тайны. Хотя подчас целью кибершпионов являются массивы информации, хранящейся в государственных автоматизированных системах и базах данных. Кибершпионы часто ставят целью кражу массива информации, подобные действия могут позволять получать большое количество персональных данных и/или коммерчески значимой информации. Их целью может быть изменение, а также удаление определенной информации, что позволяет устранить компрометирующую информацию и создать положительную историю или, наоборот, скомпрометировать лицо, создав отрицательную историю, или, к примеру, создать определенные условия для совершения противоправного действия.

Современный уровень информационных технологий и распространение так называемых «умных» устройств, с одной стороны, облегчило общение людей и позволило разговаривать через Интернет как в пределах одного региона, так и межконтинентально, а с другой стороны, открыло новые возможности в кибершпионаже, позволив прослушивать (получать звуковую информацию), а иногда и просматривать (получать визуальную информацию) с переносных портативных устройств и иного оборудования.

В настоящее время у многих граждан есть смартфоны, планшеты, ноутбуки. В каждом из этих устройств присутствует возможность установки программного обеспечения, а также есть встроенный микрофон, камера, и GPS-приемник, что позволяет, при условии наличия подключения к глобальной информационно-телекоммуникационной сети Интернет и установленного специального программного обеспечения «снимать» с устройств любую информацию (в том числе прослушивать разговоры, совершенные с данного устройства или находящиеся в пределах «слышимости» и/или «видимости» устройства).

11 июля 2014 г. Президент Российской Федерации В.В. Путин в своем интервью ИТАР-ТАСС «назвал кибершпионаж лицемерием в отношении партнеров, а также посягательством на государственный суверенитет и нарушением прав человека. Глава государства заявил о готовности РФ вместе с другими странами начать разработку системы международной информационной безопасности» [5].

Подобное заявление подчеркивает актуальность данной проблема, если даже лидер такого могущественного государства, как Российская Федерация, обратил на нее свое внимание.

На сегодняшний день заниматься кибершпионажем могут позволить себе не только государственные органы, но крупные корпорации, холдинги, а также частные разведывательные организации. При этом особенно важно то, что подчас многие из них даже не приступают закон, при этом, по сути, существенно умаляют права человека и гражданина, компании и т.д.

По мнению автора, подобную ситуацию возможно переломить только путем комбинаций осмысленных высокопрофессиональных действий в данной сфере. Возможные меры могут включать:

1) создание концепции национальной информационной безопасности Российской Федерации. Данная концепция может являться составной частью Концепции национальной безопасности Российской Федерации или являться отдельным нормативно-правовым актом;

2) активизацию и систематизацию работы по международно-правовому регулированию глобальной информационно-телекоммуникационной сети Интернет и ее национальных сегментов;

3) принятие государственной программы по привлечению органов государственной власти субъектов Российской Федерации в обеспечение национальной информационной безопасности Российской Федерации.

ЛИТЕРАТУРА

[1] *Галушкин А.А.* К вопросу об угрозах современного информационного века. Вопросы кибершпионажа и киберконтрразведки в современных условиях // Правозащитник. — 2013. — № 2.
[2] *Бачило И.Л.* Обеспечение безопасности интернет-среды: правовые методы и толерантность отношений против киберпреступности // Право цифровой администрации в России и во Франции: сб. научных материалов Российско-Французской международной конференции. — М.: Канон-Плюс, 2014.
[3] *Чесноков Н.А.* Правовые основы информационной безопасности в современных условиях // Правовая инициатива. — 2013. — № 4.
[4] *Шеметов М.* Россия призывает разработать международную систему информационной безопасности, которая защитит лидеров от прослушки. URL: http://itar-tass.com/politika/1310699.
[5] *Яковлев В.Ф.* Публичный доклад советника Президента Российской Федерации по правовым вопросам // Правовая инициатива. — 2013. — № 2.

TO THE QUESTION OF CYBERESPIONAGE AND CYBERCOUNTERINTELLIGENCE AT THE PRESENT STAGE

A.A. Galushkin

The Department of Judicial Authority, Law-Enforcement and Human Rights Activity
Peoples' Friendship University of Russia
6, Miklukho-Maklaya st., Moscow, Russia, 117198

In the present article the author analyzes the threat of cyberespionage caused by a wide circulation of information technologies, analyzes possible methods counteraction.

Key words: cyberespionage, threats, information security, national security, cybercounterintelligence.

REFERENCES

[1] *Galushkin A.A.* K voprosu ob ugrozax sovremennogo informacionnogo veka. Voprosy kibershpionazha i kiberkontrrazvedki v sovremennyx usloviyax // Pravozashhitnik. — 2013. — № 2.
[2] *Bachilo I.L.* Obespechenie bezopasnosti internet-sredy: pravovye metody i tolerantnost' otnoshenij protiv kiberprestupnosti // Pravo cifrovoj administracii v Rossii i vo Francii: sb. nauchnyx materialov Rossijsko-Francuzskoj mezhdunarodnoj konferencii. — M.: Kanon-Plus, 2014.
[3] *Chesnokov N.A.* Pravovye osnovy informacionnoj bezopasnosti v sovremennyx usloviyax // Pravovaya iniciativa. — 2013. — № 4.
[4] *Shemetov M.* Rossiya prizyvaet razrabotat' mezhdunarodnuyu sistemu informacionnoj bezopasnosti, kotoraya zashhitit liderov ot proslushki. URL: http://itar-tass.com/politika/1310699.
[5] *Yakovlev V.F.* Publichnyj doklad sovetnika Prezidenta Rossijskoj Federacii po pravovym voprosam // Pravovaya iniciativa. — 2013. — № 2.