ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯГЛОБАЛЬНОЙ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ» И ЕЁ РОССИЙСКОГО СЕГМЕНТА

Галушкин Александр Александрович
кандидат юридических наук, доцент, заведующий кафедрой гуманитарных, социальных, экономических и информационно-правовых дисциплин
МИИГУ им. П.А. Столыпина

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 (далее – РуНЕТ) за многие годы слабого правового режима возникла среда с очень низкой правовой культурой и во многих проявлениях режимом 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» [2. 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 подчас невозможно установить, кто именно разработал то или иное программное обеспечение для проведения разведывательных действий в сфере высоких технологий (кибершпионаж). 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 для осуществления кибершпионажа, что зачастую затрудняет, а иногда делает невозможным идентификацию лиц, осуществляющих кибершпионаж, и как результат возможности привлечения лиц к установленной форме 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 часто встречающегося мнения о том, что объектами нападения в кибершпионаже являются международные, межгосударственные, государственные органы, организации и учреждения, на самом деле объектами также часто являются и коммерческие компании и предприятия, однако по каким-то причинам,

часто этому не уделялось должного внимания, особенно в случаях, если это не было связано с хищением государственной тайны.

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 определённой 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 другого противоправного действия.

Зачастую, в «условиях глобализации, когда информационные финансовые отношения не знают территориальных границ, а международных соглашений о пределах юрисдикций государств все еще нет» [3. С. 236-237] кибершпионы стремятся похитить финансовую информацию. Целью хищения подчас становяться отнюдь не сами денежные средства, а информация (к примеру, не опубликованный годовой отчет), которая может позволить, к примеру, сыграть на акциях компании.

Принимая во внимание то, что благоприятное состояние «информационной жизни общества является условием, без которого невозможно ожидать социально-полезного результата от идеи и процессов формирования информационного общества» [1. С. 25-32], а также тот факт, что «в качестве новых угроз экономической безопасности в условиях информационной экономики» все чаще рассматривается «кибершпионаж» [4. С. 28] необходимо создание адекватного комплекса механизмов по своевременному выявлению киберугроз, а также адекватные организационные и правовые механизмы при их выявлении.

ЛИТЕРАТУРА

[1] Бачило И.Л. О законодательстве в информационной сфере отношений // Информационное общество. 2001. № 4.

[2] Бачило И.Л. Право и закон: Инфокоммуникативный аспект // Труды Института государства и права Российской академии наук. 2013. № 4.

[3] 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.

[4] Ческидов М.А. Влияние развития информационной экономики на экономическую безопасность государства // Вестник Саратовского государственного социально-экономического университета. 2013. № 3.