Всероссийский научно-практический журнал "Человек. Государство. Право"
ISSN 2311-8075, ЭЛ № ФС 77 – 55974, http://www.pslrf.ru
№ 2/2016

А.А. Галушкин
Российский университет дружбы народов

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННОЙ СРЕДЫ ДЛЯ ОСУЩЕСТВЛЕНИЯ КИБЕРШПИОНАЖА

Во втором случае могут использоваться различные методы для хищения индивидуальных данных доступа пользователя (логин, пароль, и др.) непосредственно у интересуемого объекта (к примеру с персонального компьютера в процессе ввода), или иным способом, при этом получение указанных индивидуальных доступа могут позволить получить информацию о данном конкретном лице.

Каждый из указанных методов является эффективным и целесообразным для применения в каждом конкретном случае. Однако, первый метод, в отличие от второго, как правило, значительно более сложен и требует от лица, а, как правило, группы лиц его реализующего существенно большей подготовки и материально-технической базы. Каждый из указанных методов имеет свои особенности, однако методы являются весьма эффективными, а главное в своем большинстве доступны значительному кругу лиц.

Как справедливо отметила профессор Бачило И.Л., "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" [1].

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.

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» [2. 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» [3], 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.

Необходимо понимать, что сама «киберугроза может быть как неумышленной, так и намеренной, нацеленной или ненацеленной, и она может исходить из множества различных источников, включая иностранные государства, осуществляющие шпионскую деятельность и информационные войны, преступники, хакеры, создатели вирусов, определенные сотрудники и подрядчики, работающие в организации» [5. С. 119]. В зависимости от указанных особенностей необходимы различные подходы.

ЛИТЕРАТУРА

[1] Бачило И.Л. Обеспечение безопасности интернет-среды: правовые методы и толерантность отношений против киберпреступности // Сборник научных материалов Российско-Французской международной конференции "Право цифровой администрации в России и во Франции", 2014.

[2] 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.

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

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

[5] Ghari W., Shaabi M. Cyber Threats In Social Networking Websites // International Journal of Distributed and Parallel Systems. 2012. Vol. 3, Iss. 1.