чатка информации с него могут содержать разные по полноте объемы фактографических данных, значимых для исследования обстоятельств при рассмотрении дела.

В сети в настоящее время рекламируются различные интернет-сервисы, ориентированные на превентивную защиту интеллектуальной собственности и прав авторов. Фирмы готовы предоставить своим клиентам экспертное заключение о подлинности, дате и времени регистрации ими данных, которое теоретически может быть использовано заявителем в суде. Однако оценка легитимности такого экспертного заключения и принятие его в качестве доказательства – сегодня полностью в компетенции суда. Вопрос будет заключаться в признании судом равнозначности в качестве доказательств юридической силы протокола, составленного нотариусом и сохраненного в бумажном варианте, и в электронном формате информационного образа факта события и его состава, заверенного ЭЦП удостоверяющего центра и депонированного им.

А.В. Казеев, Т.Г. Чудиловская

ОБ ОПРЕДЕЛЕНИИ ПОНЯТИЯ «ИНФОРМАЦИОННАЯ ВОЙНА»

Важнейшими целями развития цивилизации на различных этапах ее существования было достижение все более высокого уровня жизни, обеспечения благополучия и безопасности. Особенностью нынешней ситуации в мире является развитие информационных технологий, глобальных систем мобильной связи, взаимозависимость информационной инфраструктуры и основных важных для национальной безопасности инфраструктур (энергетической, телекоммуникационной, транспортной, банковско-финансовой, административной). По мировым телекоммуникационным сетям и через средства массовой информации осуществляется глобальная информационно-культурная и информационно-идеологическая экспансия Запада. Благодаря современным коммуникационным технологиям виртуальная реальность, создаваемая СМИ, часто становится более правдоподобной, привлекательной и достоверной в глазах массовой аудитории, чем подлинная реальность. Поэтому актуальной является проблема не только защиты национальных информационных ресурсов, но и защиты от разрушающего воздействия информации, приобретающей международный масштаб и стратегический характер.

В современных условиях обеспечение информационной безопасности личности, общества, государства и мирового сообщества, противодействие информационно-психологическому давлению и шантажу приобретает огромное значение.

В последнее время все более прочно входит в обиход понятие информационной войны, включающей любые действия, направленные на завладение важной информацией, нарушение нормального функционирования информационных систем, затруднение работы для санкционированных пользователей, разрушение банков и баз данных, незаконное проникновение в информационные сети, уничтожение информации, содержащей в компьютерах и информационных сетях, предоставление противоборствующей стороне ложной информации, распространение слухов, дискредитирующей информации, а также информации, ставящей под сомнение идеологические и духовные принципы, распространение угроз и т. д.

До настоящего времени и в методологических документах, и в нормативных правовых актах, и среди специалистов не выработано единое понимание термина «информационная война».

Обращаясь к научному определению данного понятия, необходимо упомянуть, что первоначально некто Томас Рона использовал его в отчете, подготовленном им в 1976 г. для компании Boeing, и назвал «Системы оружия и информационная война». Т. Рона указал, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время она становится и уязвимой целью как в военное, так и мирное время. Этот отчет и можно считать первым упоминанием термина «информационная война».

Анализируя предпосылки и механизмы ведения информационных войн, А.С. Горохов определяет информационную войну как действия (деятельность) государств (их блоков) по достижению своих целей в отношении других государств (их блоков), осуществляемые преимущественно невоенными средствами с использованием информационного оружия [1, с. 231].

В нормативных правовых актах Республики Беларусь только в подпрограмме «Организация системы обеспечения безопасности информационных космических технологий», утвержденной постановлением Совета министров Республики Беларусь от 14 октября 2008 г. № 1517 «О национальной программе исследования и использования космического пространства в мирных целях на 2008–2012 годы», делается ссылка на то, что способ воздействия человека на информационные системы является либо получение выгоды от обладания информацией, либо причинение материального ущерба вследствие уничтожения (разрушения) информации (военные действия, терроризм, информационные войны).

Легальное определение понятия «состояние войны» дается в законе Республики Беларусь от 3 ноября 1992 г. «Об обороне». Так, в ст. 1

отражено: состояние войны – отношения между Республикой Беларусь и другим государством (другими государствами) с момента объявления другим государством (другими государствами) войны Республике Беларусь, нападения на Республику Беларусь со стороны другого государства (других государств) или же объявления Республикой Беларусь войны другому государству (другим государствам) до заключения мира между воюющими сторонами».

Исходя из данного определения, можно произвести отграничение между информационной войной и войной обыкновенной. Во-первых, информационная война не требует ее объявления противнику, а, наоборот, ведется так, чтобы он об этом ничего не заподозрил. Во-вторых, следует отметить тот факт, что военные действия, т. е. ведение обычной войны, не исключают ведения войны информационной, о чем свидетельствует война в Южной Осетии в 2008 г. Данный пример является классическим, так как показывает превосходство информационной войны над обычной.

Если вспомнить те не столь давние события, то сами военные действия не имели такой продолжительности, как борьба в информационной войне между Россией и Западом, при этом победа на полевом фронте не означала победу на информационном. Информационное пространство, в котором ведется информационная война, динамично: в нем не бывает завершенного состояния. Из этого можно сделать вывод о достаточно трудном достижении постоянного информационного доминирования.

Изложенное является лишь частным фрагментом важной проблемы обеспечения информационной безопасности в эпоху информационных войн и требует дальнейшего исследования. Следует отметить, что в качестве инструментов исследования информационных войн используются системный подход и теория управления эволюцией организации. С их помощью разработаны базовые адаптивные механизмы информационных войн. Комбинации этих механизмов необходимы для анализа и проектирования комплексных систем управление информационными войнами разного уровня и масштаба [2, с. 12].

Принимая во внимание мнения таких специалистов, как С.Н. Гриняев, М.В. Ильин, А.А. Мухин, В.А. Лисичкин, Г.Г. Почепцов, С.П. Расторгуев, В.В. Цыганков, В.Н. Шелепин, можно сделать вывод, что информационная война – комплекс явных и скрытых целенаправленных мероприятий по информационному воздействию на массовое сознание для изменения поведения людей, с целью достижения информационного превосходства в обеспечении национальной военной стратегии или получения иной материальной выгоды, а также защита от подобных воздействий.

1. Горохов А.С. О содержании понятий «информационная безопасность», «информационная война» и «информационное оружие» // Управ. защитой информ. 2004. Т. 8, № 2. С. 229–233.

2. Цыганков В.В., Бухарин С.Н. Информационные войны в бизнесе и политике: Теория и методология. М. : Акад. проект, 2007.

Е.Т. Капитанец

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В МЕЖДУНАРОДНОМ ИНФОРМАЦИОННОМ ПРАВЕ

В условиях рыночной экономики информационные ресурсы приобретают высокую, особую ценность в связи с выступающим фактором конкуренции. Побеждает тот, кто качественнее, дешевле и оперативнее производит и продает. Кто владеет информацией – тот владеет миром.

Ведущая роль в процессах глобализации отводится информационным технологиям (ИТ), дающим возможность:

улучшить качество исходного продукта, т. е. ИТ помогают в принятии объективных решений на международном уровне;

сократить регламент времени на выработку этих решений;

оперировать достоверной информацией;

увеличить скорость ее распространения адресатам.

Можно выделить на мировом уровне два аспекта функционирования сферы информационных технологий:

1. Информационные технологии – мощнейший и эффективнейший инструмент межгосударственных экономических, гуманитарных, в том числе правовых отношений.

2. Информационные технологии – определенная сфера бурно прогрессирующих человеческих отношений.

В силу реалий существования второго аспекта возникла необходимость правового урегулирования данного рода человеческой деятельности – создания международного правового поля для эффективности и безопасности информационных технологий, систем, в том числе безопасности получаемой информации потребителем продукта ИТ. Имеется в виду группа норм международного характера с определенной организующей дефиницией – Международное информационное право.

Принимая во внимание второй аспект нашего подхода, можно отметить, что правом необходимо регламентировать практически все сферы компьютерных информационных технологий, например:

коммуникационные сети и системы передачи информации;

информационные сети (глобальные, специализированные, региональные) и их дифференциацию и интеграцию;

информационную безопасность и прозрачность информационных ресурсов и т. д.