ная и на персональных компьютерах, и на компьютерах, соединенных как в локальную, так и в глобальные информационные сети. Эти виды преступлений вошли в отдельный раздел Уголовного кодекса Республики Беларусь «Преступления против информационной безопасности».

Компьютерная преступность стала настоящим бичом экономики развитых государств. Так, например, 90 % фирм и организаций в Великобритании в разное время становились объектами электронного пиратства или находились под его угрозой, в Нидерландах жертвами компьютерной преступности стали 20 % различного рода предприятий. В ФРГ с использованием компьютеров ежегодно похищается 4 млрд евро, а во Франции – 1 млрд евро.

Наибольшую общественную опасность представляют преступления, связанные с неправомерным доступом к компьютерной информации. Известно, рассматриваемые правонарушения имеют очень высокую латентность, которая по различным данным составляет 85–90 %. Более того, факты обнаружения незаконного доступа к информационным ресурсам на 90 % носят случайный характер.

Анализ материалов отечественных уголовных дел позволяет сделать вывод о том, что основными причинами и условиями, способствующими совершению компьютерных преступлений, в большинстве случаев стали:

1) бесконтрольность за действиями обслуживающего персонала, что позволяет преступнику свободно использовать ЭВМ в качестве орудия совершения преступления;

2) низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

3) несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

4) отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации;

5) отсутствие категорийности допуска сотрудников к документации строгой финансовой отчетности;

6) отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации.

Для эффективной защиты от компьютерных преступлений и утечки служебной информации на факультете внутренних войск был выполнен ряд мероприятий:

1) просмотрена вся документация;

2) определены возможные каналы утечки информации;

3) ликвидированы слабые звенья в защите;

4) определены категории допуска для лиц, имеющих право доступа;

5) определена дисциплинарная ответственность за сохранность и санкционированность доступа к имеющимся информационным ресурсам;

6) организован периодический системный контроль качества защиты информации посредством проведения регламентных работ как самим лицом, ответственным за безопасность, так и с привлечением специалистов;

7) проведена классификация информации в соответствии с ее важностью;

8) определено должностное лицо, отвечающее за режим секретности и конфиденциальности информации;

9) обновлено защитное программное обеспечение.

Таким образом, на факультете внутренних войск на высоком уровне осуществляется защита и предупреждение утечек служебной информации, защита от возможности компьютерной преступности, совершенствование программного обеспечения.

УДК 343

В.Ю. Арчаков, О.С. Макаров

ПРАВОВЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Заканчивается второе десятилетие XXI в. Наряду с такими вызовами человечеству, как потепление климата, истощение природных ресурсов, мы рассматриваем угрозы, вызванные глобальным процессом информатизации нашей цивилизации.

В связи с тем, что современное общество переместило свои социальные отношения в информационную среду, где традиционные, выработанные тысячелетиями регуляторы безопасности не действуют, а адекватные системы их защиты в информационной сфере пока не разработаны, социум претерпевает негативные последствия реализации информационных угроз: растет информационная преступность, на личность оказывается деструктивное информационное воздействие, развивается кризис тайн и т. д.

В обозначенных условиях рельефно проявляется дилемма: обозримый путь общественного развития пролегает через процессы информа-

тизации, однако информатизация общества порождает геометрическое возрастание угроз национальной безопасности.

Информационная сфера становится доминантой в структуре национальной и международной безопасности. Информация выступает сегодня как предмет деятельности и объект защиты, как источник опасности и как оценочный индикатор безопасности общества и всех его институтов.

По мере развития социума информация превратилась в высокоэффективное оружие, с помощью которого решается широкий спектр задач в экономической, политической и в военной сферах. Возникшие глобальные информационные поля оказались способными воздействовать на людей, не взирая на государственные границы, создавать возможность манипуляции сознанием в планетарном масштабе. Факты свидетельствуют, что духовная сфера – сознание и ценностные ориентации людей – оказалась наиболее уязвимой областью национальной безопасности. Распространение посредством СМИ, а также социальных сетей недостоверной или умышленно искаженной информации способно спровоцировать не только массовые беспорядки в обществе, но и обвал экономической и финансовой систем государства.

Основным угрозообразующим для информационной безопасности фактором во втором десятилетии XXI в. стал нарастающий дисбаланс между прорывным насыщением потребностей социума технологиями информатизации и ощутимым отставанием в организации использования информационного ресурса общества. Цифровая эпоха сделала первые шаги в технологическом направлении, но испытывает сложности в синхронизации интересов акторов и обеспечении их безопасности.

Еще одним побочным эффектом технологического прогресса становятся негативные факторы социального, культурного, экономического планов (киберпреступность, кибертерроризм, информационные войны и др.), питательной средой которых среди прочих выступает информационное, цифровое неравенство, правовая неопределенность и безнаказанность. Это затрудняет определение правовых, политических, этических параметров отношений как внутри государств, так и в их сообществах, а также в решении проблем общемирового значения.

Для продолжения развития информационного общества необходимо обеспечить эффективное противодействие угрозам использования современных информационных технологий для нарушения мира и безопасности, совершения преступлений, подготовки и осуществления террористических актов, распространения террористической идеологии и практики разрешения противоречий общественного развития. Данная работа в силу трансграничности угроз информационной безопасности

должна проводиться на национальном уровне и с позиций международного взаимодействия.

Представляется, что решение указанных проблем находится не в технической, а в социальной плоскости, а значит, предполагает осознание обществом новых, обусловленных процессами информатизации условий социальной жизни и выработку определенных правил безопасной межличностной, общественной, государственной и межгосударственной коммуникации с последующим их юридическим закреплением и формированием соответствующего механизма защиты складывающихся отношений.

За последние 15 лет произошло значительное расширение сферы информационной безопасности и увеличение методов ее обеспечения, что связано с пониманием недостаточности методов защиты и охраны информационных ресурсов. Границы информационной безопасности позволяют информации быть открытой и доступной и влиять на все слои и группы пользователей.

В этих условиях особую роль в обеспечении информационной безопасности призвано исполнить право, именно взаимодействие в рамках правовых систем разных государств и отраслей законодательства. Нормативно-правовая основа необходима для поддержания стратегической стабильности и развития партнерства во всех областях жизни общества и одновременно для создания условий формирования безопасного информационного общества.

В то же время в области современного правового регулирования сферы информационного взаимодействия складывается ситуация напряжения, что предопределяет поиск решений по оздоровлению информационной среды, особенно интернет-среды, обеспечению информационной безопасности.

В силу трансграничного характера информационных отношений на первый план правового обеспечения информационной безопасности выступает международное право.

Критический взгляд на современное состояние правового обеспечения информационной безопасности на международном уровне позволяет сделать вывод о его концептуальной неопределенности. Правовое регулирование в данной сфере очевидно поверхностно, так как постоянно лавирует, решая сиюминутные политические задачи, «залатывает» социальные пробелы, вызванные скачками информатизации, и запоздало реагирует на информационные угрозы правам и интересам субъектов отношений. Локомотивом нормативного урегулирования отношений в области обеспечения международной информационной безопасности сегодня выступают документы политического характера (различные стратегии, доктрины, правила поведения, планы и т. п.).

В результате у правоведов формируются очевидные фобии нормотворчества, обуславливающие появление правовых лакун в регулировании информационной безопасности на национальном и международном уровнях.

Так, например, научное сообщество и законодатели большинства стран определились, что термины «кибербезопасность» и «информационная безопасность» не тождественны, однако в ряде нормативных актов они сосуществуют, в других конкурируют, в третьих эквивалентны друг другу.

Схожая ситуация в отношении понятий «информационная война» и «информационное оружие». Их введение (после долгих научных споров) в соглашение Шанхайской организации сотрудничества (ШОС) презентовалось как прорыв в правотворчестве. Но сегодня ряд ученых считает данные термины неудачными, не отвечающим и международной трактовке базового понятия «война». Наметилась тенденция к вытеснению их не милитаристическим понятием «деструктивное информационное воздействие».

Также представляет интерес подмена в юридически значимых документах стволового понятия «киберпреступления» политизированным термином «киберугрозы».

Кроме этого, в нормативных актах в области обеспечения информационной безопасности начал подвергаться ревизии неоспоримый примат основы основ европейской правовой модели – свобода информации. В теории, а затем в международных документах его теснит принцип баланса информационных свобод с интересами обеспечения информационной безопасности.

При этом просматривается сдержанность юристов в формулировании запретов в области обеспечения информационной безопасности (например, запрета на распространение заведомо недостоверной информации, запрета на использование информационных технологий в ущерб безопасности других лиц и т. д.).

Правовое регулирование общественных отношений в целях обеспечения информационной безопасности уверенно опирается на сформировавшиеся институты ответственности за киберпреступления и посягательства на всякого рода тайны. Остальные правила поведения формулируются в политическом ключе как «озабоченность», «порицание», «неприятие».

Складывается впечатление, что в области обеспечения международной информационной безопасности государства стараются избегать жестких правовых ограничений, оставляя правовой недосказанностью «серые зоны» для политических решений.

Обобщение современной практики правового обеспечения информационной безопасности в глобальном масштабе позволяет выделить две основные конкурирующие правовые модели, которые, исходя из географии применения, условно можно назвать европейской и евразийской.

Европейская модель основывается на конвенции Совета Европы о киберпреступности, принятой в 2001 г. в Будапеште. Она достаточно эффективно используется в ряде государств и преимущественно охватывает области деятельности, непосредственно связанные с использованием технических средств сбора, обработки, защиты, распространения и использования информации. Поэтому в рамках данной платформы оперируют такими понятиями, как «кибербезопасность», «киберугрозы», «кибератаки».

К недостаткам европейской модели, на наш взгляд, относится принципиальное отсутствие упоминаний о деструктивном информационном воздействии на сознание населения, а также умалчивание о современных инструментах совершения киберпреступлений (ботнеты, спам, фишинг и др.). Против Будапештской конвенции выступают Китай, Индия, Южная Африка, Бразилия, а также не подписавшая данный документ Россия.

Евразийская модель, в отличие от европейской, строится на более широкой трактовке угроз, и вопросы чистой кибербезопасности рассматриваются наряду и в тесной взаимосвязи с общими проблемами всей сферы массовых коммуникаций, в том числе с распространением противоправного либо нежелательного контента. Поэтому речь идет именно об информационной безопасности, а не о безопасности информации или безопасности компьютерных систем и сетей.

Евразийская модель нашла отражение в Соглашении между правительствами государств – членов ШОС в области обеспечения международной информационной безопасности, в документах ОДКБ, в Соглашении о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности и в других документах СНГ.

Антагонизм вышеназванных моделей отчетливо указывает на то, что в ближайшем обозримом будущем не следует рассчитывать на общее в глобальном смысле понимание и согласование правовых норм в сфере международной информационной безопасности. Необходимо незамедлительно совершенствовать механизмы регионального сотрудничества, выстраивая жизнеспособную систему международной информационной безопасности в рамках существующих организаций, объединений и союзов.

Сегодня на повестке для регионального взаимодействия в области обеспечения международной информационной безопасности находятся проекты Соглашения о сотрудничестве государств – членов Организа-

ции Договора о коллективной безопасности в области обеспечения информационной безопасности и Стратегии обеспечения информационной безопасности государств – участников Содружества Независимых Государств. Полагаем, принятие данных актов повысит эффективность обеспечения международной информационной безопасности.

УДК 004.42

С.С. Мишук

СИСТЕМА ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ КАК ЭЛЕМЕНТ НООСФЕРЫ

Возникновение и функционирование информационного общества, ядром которого является система инфокоммуникационных технологий, стало объективной реальностью XXI в. Различные аспекты данного явления постоянно описываются в современной литературе. Однако исследованию его в качестве необходимого и закономерного этапа эволюции как человеческого общества, так и планеты Земля в целом уделяется, на наш взгляд, недостаточно внимания. Между тем использование имеющихся в науке подходов к изучению явлений подобного типа позволило бы глубже понять специфику этого периода общепланетарной эволюции. Одной из теорий, формирующих методологическую основу анализа данной проблемы, безусловно, является учение академика В.И. Вернадского о ноосфере.

На наш взгляд, инфокоммуникационные технологии превратились на современном этапе в один из важнейших компонентов ноосферы как планетарной оболочки. Для корректного анализа их роли и значения именно в данном качестве необходимо зафиксировать, по крайней мере, две содержательных трактовки понятия «ноосфера» в трудах В.И. Вернадского.

Во-первых, ноосфера трактовалась им как определенный этап в планетарном развитии Земли.

Во-вторых, ноосфера трактовалась и как этап именно разумного преобразования той среды, в которой живет человек. В.И. Вернадский подчеркивал, что наличие сознания как необходимого компонента предметно-преобразовательной деятельности человека не означает автоматически, что данная деятельность осуществляется разумно в подлинном смысле слова. Активность человека может приводить и к нежелательным, даже опасным для него самого последствиям.

Сам факт возникновения ноосферы как принципиально новой планетарной оболочки означает также известный отрыв человека от процессов собственно земной эволюции. Именно на данном этапе человечество оказывается в состоянии преодолеть земное притяжение и покинуть пределы среды своего возникновения. Иными словами, человеческая деятельность превращается в фактор не только земной, но и космической эволюции. В подобных условиях значение именно разумности человека в самом широком смысле слова возрастает многократно. И в этом смысле ноосфера (именно как сфера разума, как разумно устроенная сфера обитания человечества) должна пониматься не только как одна из планетарных оболочек и этап земной эволюции, но и как цель будущего развития человечества. И данная цель может быть достижима при условии понимания человека уже не как чисто планетарного, земного фактора, но и как силы, которая выходит за рамки отдельной планеты и в бесконечном времени становится значимой для всей Вселенной.

В своих трудах В.И. Вернадский достаточно полно систематизировал факторы, которые необходимы для формирования и успешного функционирования и развития ноосферы. Постараемся кратко проанализировать те из них, которые непосредственно связаны с функционированием системы инфокоммуникационных технологий, – «резкое преобразование средств связи и обмена информацией» и «свобода научной мысли и научного поиска от давления религиозных, философских и политических построений».

Возникновение в конце XX в. и функционирование в современных условиях информационного общества со всей очевидностью демонстрирует значение инфокоммуникационных технологий как системообразующего элемента. Они выступают одним из важнейших факторов устойчивого существования и дальнейшего развития человеческой цивилизации.

Для изучения действительной значимости инфокоммуникационных технологий следует рассмотреть их функционирование в структуре ноосферы как уже достаточно сформированной планетарной оболочки. Раз возникнув, ноосфера начинает эволюционировать как самостоятельная система. Присущие именно ей законы приводят к необходимому появлению и последующему отбору таких механизмов, объективная потребность в которых возникает на определенном этапе развития. Причем наиболее значимые механизмы появляются чаще всего в тех структурных элементах ноосферы, которые являются сущностными для нее, то есть связанными в первую очередь с функционированием разума и знания. Возникновение подобных инновационных по своей природе элементов стимулирует прогресс человеческого общества в масштабах планеты не только опосредовано. Они непосредственно