Жатканбаева А.Е.

Об опыте правового регулирования обеспечения информационной безопасности в США и ЕС

В статье рассматривается опыт принятия и реализации законодательства Соединенных Штатов Америки и ЕвроСоюза по вопросам обеспечения информационной безопасности личности, общества и государства. Прослеживаются причины, последовательность и последствия принятия специальных законодательных актов в военной и гражданской сферах. Данный опыт исследуется в целях потенциальной возможности использования его для совершенствования информационно-правовой сферы Республики Казахстан.

Ключевые слова: информационная безопасность, информационные интересы, Интернет, средства массовой информации и коммуникации.

Zhatkanbaeva A.E.

On the experience of legal regulation of information security in the United States and the EU

In the article experience of acceptance and implementation of the legislation of the United States of America and the European Union concerning ensuring information security of the personality, society and the state is considered. The reasons, the sequence and consequences of adoption of special acts in military and civil spheres are traced. This experience is investigated for a potential possibility of his use for improvement of the information and legal sphere of the Republic of Kazakhstan.

Key words: information security, information interests, Internet, mass media and communications.

Жатканбаева А.Е.

АҚШ мен ЕО ақпараттық қауіпсіздік саласындағы құқықтық реттеу тәжірибесі туралы

Берілген мақалада мемлекет пен қоғам, тұлғаның ақпараттық қауіпсіздігін қамтамасыз ету мәселелері бойынша ЕуроОдақ пен Америка Құрама Штаттарының заңдарын жүзеге асыру мен қабылдау тәжірибесі қарастырылады. Азаматтық және әскери ортадағы арнайы заңнамалар қабылдау салдарлары, бірізділігі және себептері ескеріледі. Берілген тәжірибе оны мүмкіндік туындаған жағдайда Қазақстан Республикасының ақпараттық-құқықтық саласында қолдану үшін зерттеледі.

Түйін сөздер: ақпараттық қауіпсіздік, ақпараттық қызығушылықтар, интернет, бұқаралық ақпарат және коммуникация құралдары.

УДК 34(4/9)

Жатканбаева А.Е.

Казахский национальный университет имени аль-Фараби,
Республики Казахстан, г. Алматы
E-mail: Zhatkanbayeva.aizhan@kaznu.kz

ОБ ОПЫТЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В США И ЕС

Интерес к опыту Соединенных Штатов Америки в вопросах правового регулирования обеспечения информационной безопасности обоснован уже тем, что именно данная страна является безоговорочным лидером в этой сфере.

Роль Соединённых Штатов Америки как одного из наиболее могущественных политических, экономических и военных фигур современной международной политики в настоящее время обуславливается еще и в умении вести грамотную деятельность в области информатизации.

Именно США стали создателем Интернета и страной с наиболее распространенной трансграничной сетью и соответственно, ранее большинства других стран столкнувшейся с информационными угрозами национальной безопасности. В результате Штаты стали пионером в области разработки политики в сфере информационной безопасности, которая изначально была взята под государственное крыло.

США первыми создали государственную систему регулирования в информационной сфере, которая обеспечивает эффективное использование новейших информационных технологий для ускорения развития национальной экономики. Помимо этого, именно под государственным началом был разработан новый вид оружия – информационного, а также психологического и психотропного воздействия. Государственная информационная система США продолжает развиваться и включает в себя: «законодательную основу, обеспечивающую органы государственной власти большими полномочиями в информационной сфере, организационные структуры, в функции которых входит противодействие информационным угрозам, расследование информационных преступлений, использование ИТ для обеспечения позиций США на международной арене. В американской государственной системе обеспечения информационной безопасности сложилось своего рода государственного частное партнерство правоохранительных, военных и разведывательных органов, а также бизнеса» [1, с. 7].

Основу такой политики заложили в период правления Кенеди. Уже в середине 90-х годов правительство столкнулось с проблемой роста киберпреступности, которая при этом по-

казывала безграничный потенциал. Но при этом политологи отмечали, что принимаемые в этот период административные и нормативные меры не были столь радикальными и не решали существующих проблем и тем более не были направлены на перспективу. И только «11 сентября 2001 г. продемонстрировали серьёзную уязвимость системы национальной безопасности страны и послужили поводом для значительных изменений в этой сфере. Объявленный принцип превентивных действий в принятой в 2002 г. Стратегии национальной безопасности США требовал создания системы обеспечения вооружённых сил оперативной, точной и наиболее полной информацией не только о врагах, но и о любых потенциальных угрозах национальной безопасности США» (Шариков). Именно тогда были произнесены официальные слова Дж. Буша: «Нация в опасности, наше общество представляет собой практически бесконечный набор потенциальных целей, удар по которым может быть нанесен различными методами».

Впервые вопрос о необходимости пересмотра стратегии обеспечения внутренней безопасности в новейших условиях был поднять в конце 90-х. Но сам акт был принят только после теракта 11 сентября, что существенно повлияло на его содержание и на само определение понятия «внутренняя безопасность», важнейшим направление которого была признана защита кибер-пространства. Хотя Закон о внутренней безопасности был принят еще 25 ноября 2002 года, в соответствии с которым в январе 2003-го Агентство Внутренней Безопасности было преобразовано в Министерство внутренней безопасности (МВБ).

В. Пашков, анализируя работу данного органа, отмечает, что одной из задач, поставленных перед МВБ, была задача анализа информации и защиты инфраструктуры следующих подразделений министерств и ведомств правительства США. В штат министерства вошли в том числе: Национальный центр защиты инфраструктуры при ФБР Министерства юстиции (National Infrastructure Protection Center-NIPC), Национальный центр моделирования и анализа инфраструктуры при Институте проблем защиты информационной инфраструктуры Министерства энергетики (National Infrastructure Simulation and Analysis Center – NISAC), Федеральный центр защиты информационных ресурсов администрации общих служб (Federal Computer Incident Response Center of the General Services Administration – FedCIRC), Управление безопасности энергетических систем Министерства энергетики (Energy Assurance Office of the Department of Energy – EAO), Национальная система связи МО (National Communication System – NCS) а также подразделение кибернетической безопасности (National Cyber Security Division – NCSD), главным элементом которого является вновь образованный за счет объединения трех групп немедленного реагирования (CC/CERT, NCS, NTPC) Центр экстренного реагирования на компьютерные происшествия в США (U.S. Computer Emergency Response Team – US-CERT) [2].

В 2008 году были введены в действие две секретные директивы – № 54 (по национальной безопасности) и № 23 (по внутренней безопасности), в соответствии с которыми спецслужбам были даны полномочия по усилению контроля за компьютерными сетями, используемыми американскими федеральными структурами, а также расширить мониторинг информации, поступающей в сети правительственных органов Соединенных Штатов через Интернет. И только после 2011 года на официальном уровне было признано, что контроль над секретными коммуникациями противника при одновременной защите своих собственных предоставляет им уникальные возможности для сохранения лидирующих позиций в мире.

Были введены новые стандарты информационной безопасности, при которых существенно увеличились возможности государства в области контроля и регулирования информационной сферы, в том числе и за частной жизнью американцев. А также был принят ряд законодательных актов, обеспечивающий её правовую основу, прежде всего Закон о борьбе с терроризмом, который получил название «Акт Патриот», и был инициирован проект «Тотальная информационная осведомлённость», позволявший привлечь информационные ресурсы министерства обороны для массового шпионажа над гражданами. По данным ФАПСИ, расходы США за последние 15 лет на разработку и приобретение средств информационной борьбы выросли в 4 раза и занимают ныне первое место среди расходов на все военные программы, тогда как американские военные расходы составляют 40% расходов на оборону всех стран мира. Еще выше американская доля в глобальных расходах на закупку вооружений (около 65%) и на военные НИОКР (примерно 75%) [3].

Вместе с тем, существенно изменилась внешняя политика США в информационной

сфере, чему свидетельствуют приведенные в данном исследовании примеры о международных скандалах о прослушке глав государств и рядовых иностранных граждан. Политика США на установление глобального информационного контроля в глобальном масштабе была внедрена и существенно продвинута Бараком Обамой, который уже в первом своем докладе, посвященном первым сто дням своего правления, был сделан вывод о приоритетности обеспечения информационной безопасности путем усиления государственного регулирования в области обеспечения информационной безопасности и развития информационных технологий.

При этом следует отметить, что такая политика встретила существенное сопротивление правозащитных организаций, которые подвергли жесткой критике деятельность американского правительства, создающего все необходимые условия для технического и правового сопровождения деятельности органов национальной безопасности США на беспрепятственное получение любой необходимой информации, в том числе частного характера.

При этом следует отметить в качестве важнейшего аспекта в политике администрации Б. Обамы в сфере обеспечения информационной безопасности еще более тесное сотрудничество государства и бизнеса, направленное на защиту государственных информационных ресурсов и всего американского информационного пространства, что в первую очередь реализовывается путем государственного поощрения научно-технического прогресса. «Фундаментальные достижения в области знаний официально признаны в качестве основы экономического роста, поскольку согласно имеющимся в США оценкам на 1 доллар, вложенный в НИОКР, приходится 9 долл. роста ВВП. Роль правительства США отныне сконцентрирована на поддержке перспективных гражданских технологий будущих поколений, несущих в себе будущее научно-технического потенциала страны в XXI веке. Это приоритетное направление государственной научно-технологической политики наравне с крупными военно-техническими программами. Ежегодно США расходуют на информационные технологии только из федерального бюджета порядка 38 млрд. $, из которых около 20 млрд. $ (более 50%) составляют расходы военного ведомства» [4].

Нельзя не отметить и тот факт, что США первая и сильнейшая страна в сфере использования информационного оружия и развертывания информационных воин. Так, анализируя использование Соединенными Штатами Америки средств массовой информации и коммуникации в качестве инструмента внешнеполитических акций, Щербакова Т.В. считает, что это «в корне изменило «правила» проведения военных операций. Если до 1990-х годов успех зависел от полной секретности подготовительной стадии и внезапности начала вооруженных действий, то теперь именно широкая огласка и обсуждение в прессе планируемой военной операции США – залог победы». Технологии информационной борьбы не раз использовались США в различных международных конфликтах. После окончания войны в Персидском заливе (военной операции «Буря в пустыне») США впервые открыто заявили о широкомасштабном использовании информационного оружия в ходе боевых действий. В отношении вооруженных сил и населения Ирака, а также населения США и других стран применялись методы психологического воздействия, направленные, с одной стороны, на моральное подавление противника и, с другой стороны, на формирование положительного отношения в мире к действиям американских военных. Главной задачей ВКМ во время проведения военных операций было такое управление информационным потоком, которое вводило в массовое сознание структуры с заранее прогнозируемой системой реакции на них. Это все существенней проявляется в военных акциях с участием США к концу 1990-х годов, логическим развитием данного направления внешнеполитического коммуникационного менеджмента стала выработка стратегии «экспорта революций», проявившая себя уже в XXI веке, в Сербии в 2000 году, в Грузии в 2003 году и на Украине в 2004 году» [5]. Сегодня можно добавить и новые примеры – Ирак, Сирию, Египет и Украину 2014 года.

Достаточно схожа с позицией США политика Великобритании – давнего союзника и партнера.

В 2008 году Премьер-министр Великобритании Гордон Браун представил парламенту новую Стратегию национальной безопасности, в соответствии с которой граждане должны принимать активное участие в обеспечении национальной безопасности. В 2010 году был создан Национальный совет безопасности (National Security Council, NSC) Великобритании, в целях оптимизации усилий в сфере безопасности и международной политики.

Стратегия национальной безопасности определила «национальный реестр потенциальных рисков», в числе которых информационная безопасность заняла главенствующее место. Была существенно преобразована деятельность Комитета по разведке и безопасности, который был создан согласно Закону «О разведывательных службах» (1994) и теперь включает в себя три спецслужбы: Секретной службы (MI5), разведки SIS и центра правительственной связи GCHQ. Комитет отчитывается напрямую перед премьер-министром при консультациях с лидером оппозиции.

Серьезное внимание уделено вопросам обеспечения защиты государственных секретов, которые находятся под надзором Управления безопасности аппарата Кабинета министров Великобритании, частично – Центра правительственной связи (главным органом Великобритании в сфере криптографии и защиты правительственной информации).

Политика защиты правительственной секретной информации в Великобритании в настоящее время определяется руководством Security Policy Framework (SPF), который содержит основные принципы безопасности и руководство по управлению безопасностью и рисками для государственных учреждений Великобритании и связанных с ним органов. SPF включает порядка 70 рекомендаций в области политики информационной безопасности, сгруппированных по 7 разделам: Управление, включая управление рисками; контроль доступа и засекречивание информации; персонал, ответственный за инфобезопасность; обеспечение информационной безопасности; физическая безопасность; борьба с терроризмом; непрерывность бизнеса.

Огромное внимание уделяется в Великобритании вопросам коммуникации и связи с общественностью, которую также рассматривают как национальный приоритет. В свое время Премьер-министром Блеером было сформировано Агентство правительственной информации и коммуникации – АПИК (Governmental Information and Communication Service – GICS), главным структурным образованием которого стал Комитет стратегических коммуникаций – КСК (Strategic Communication Unit – SCU), который определяет информационные приоритеты и решает, какую информацию правительство должно предоставить общественности. «В новую структуру АПИК входит подразделение, которое проводит соответствующую работу с фокус-группами и раз в неделю предоставляет данные на обсуждение в КСК. Еще одно исследовательское подразделение, совместно с департаментами министерств, занимается поиском и обнародованием т.н. «фактов-убийц» («killer-facts»). Исследовательская группа ищет факты по наиболее актуальным и востребованным со стороны общественности вопросам и по мере их нахождения посредством «сети знаний» (компьютерная сеть и программные продукты для информационного обмена, а также пейджеры, имеющиеся у каждого члена правительства) распространяет среди членов правительства и парламента. Комитет стратегических коммуникаций выполняет также функцию согласования стиля и времени опубликования информации всех правительственных структур» [6].

Страны западной Европы также стараются не отставать от того темпа правового регулирования информационной сферы, который изначально был задан США. Но тут своя специфика, анализ которой также необходим. В отличие от США и Англии, страны Западной Европы не отличаются столь агрессивным подходом, в том числе и в информационной сфере и направлены в большей степени на охранные функции.

В связи со сложившимися историческими и политическими условиями Евросоюз объединяет свои усилия в области коллективной безопасности.

Коллективная безопасность по-разному определяется в доктрине. К примеру, Н.А. Комлева полагает, что «система коллективной безопасности – это юридически оформленный союз государств, заключенный для отражения общей геополитической угрозы» [7]. О.О. Хохлышева приводит следующее определение: «Коллективная безопасность представляет собой совокупность совместных мероприятий государств и международных организаций по предотвращению и устранению угрозы международному миру и безопасности, пресечению актов агрессии и других нарушений мира. Юридически система коллективной безопасности оформлена международными договорами» [8].

Именно договорное право лежит в основе современной политики безопасности, в которой тесно взаимосвязаны все страны Евросоюза, в центре которого находится Германия.

Согласно официальной позиции, риски и угрозы современной Европе носят комплексный характер и к ним относятся:

– международный терроризм;

– распространение оружия массового уничтожения и средств его доставки;

– наличие очагов кризисов и конфликтов в Европе и за ее пределами;

– информационную войну в самых различных ее формах.

Европа уделяет огромное внимание развитию информационного общества, которая учредила Форум для обсуждения общих проблем становления информационного общества. Его цель – проследить процесс становления информационного общества в областях: воздействие на экономику и занятость; создание социальных и демократических ценностей в «виртуальном обществе»; воздействие на общественные, государственные службы; образование, переквалификация, обучение в информационном обществе; культурное измерение и будущее СМИ; устойчивое развитие, технология и инфраструктура. Кроме того, резолюция обязала каждую страну иметь концепцию формированию национальной политики в целях построения информационного общества.

Отношения в области регулирования информационных правоотношений в большей степени регламентированы различного рода директивами, которые представляют собой новую «категорию правовых актов, ранее не известную международному праву. Специфика директивы в ее обязательности для государств-членов, для действия директивы в этих государствах не требует ее утверждения (принятия) органами власти государства. Другое отличие директивы от договора в том, что она является односторонним актом. Своеобразие директивы в том, что с ее помощью задачи сообщества реализуются внутригосударственными средствами» [9, с. 10].

Хартия Европейского Союза об основных правах 2007 г. включила в каталог основных прав граждан ЕС право на защиту персональных данных Хартия Европейского Союза об основных правах (2007/C303/01) [10].

Если рассматривать специальные акты в области информационной безопасности ЕС, то необходимо вспомнить такие документы, как Резолюция 41/68 от 03.12.1986 г. «Вопросы, касающиеся информации», Резолюция от 55/63 от 04.12.2000 г. «Борьба с преступным использованием информационных технологий», Резолюции 60/45 от 08.12.2005 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», Директива от 25 нояб. 2009/136/ЕС «О конфиденциальности и электронных средствах связи», Директива от 7 марта 2002 г. 2002/22/ЕС «Об универсальных услугах и правах пользователей в отношении сетей электронных коммуникаций и услуг» и многие другие.

Евросоюзом была принята принята Стокгольмская программа, закрепляющая приоритеты развития ЕС в сфере законности, свободы и безопасности на период 2010-2014. В ней было отмечено, что информационная безопасность становится предметом заботы мирового сообщества и сформулирована задача о выработке комплексной стратегии внутри ЕС.

Кроме того, ЕС стал участником целого ряда договоров, например Соглашения о сотрудничестве в деле противодействия преступлениям в сфере компьютерной информации и компьютерному терроризму в рамках Организации договора о коллективной безопасности, Соглашение о региональной системе обеспечения безопасности информационного пространства государств-членов НАТО и ряд других соглашений. Это свидетельствует о том, что в сфере информационной безопасности началось формирование региональных систем международной информационной безопасности [11].

Литература

1 Шариков П.А. Политика США в области информационной безопасности: автореф. на соиск. уч. степ. канд. полит. наук. – М., 2009. – С. 25.

2 Пашков В. Информационная безопасность США // Зарубежное военное обозрение. – №10. – 2010. – С. 3-13.

3 Грачева В.Т. Основы могущества США // http://www.km.ru/referats/E5DD6DA3EF3543C3B1ADA9967F350E01

4 Роговский Е.А. США: информационное общество (экономика и политика). – М.: Издательство: Международные отношения, 2012. – 408 с.

5 Щербакова Т.В. Коммуникационный менеджмент во внешней политике США в конце XX века: автореф. на соиск. уч. степ. канд. истор. наук. – М., 2006. – С. 25.

6 Сагагелян А. К вопросу о проблемных аспектах информационной политики государства // Проблемные аспекты государственной информационной политики стран переходного периода. Материалы Всероссийской научно-практической конференции. – Киров, 2010. – Т. II. – С. 181.

7 Комлева Н.А. Коллективная безопасность на современном этапе // [Электронный ресурс]. – Режим доступа: http://www.roman.by/r-89725.html.

8 Хохлышева О.О. Всеобъемлющая безопасность и ее международно-правовое обеспечение в условиях глобализации // Вестник Нижегородского университета им. Н.И. Лобачевского. 2012. – № 3(1). – С. 323-331.

9 Глотова С.В. Директивы Европейского Сообщества: автореф. дис. … к.ю.н.: 12.00.10. – М., 1999. – С. 25.

10 Европейский Союз: основополагающие акты в редакции Лиссабонского договора с комментариями / отв. ред. С.Ю. Кашкин. – М., 2010. – С. 554-570.

11 Федоров А.В. Информационная безопасность в мировом политическом процессе. – М., 2006. – С. 183.

References

1 Sharikov P.A. Politika SShA v oblasti informacionnoj bezopasnosti // Avtoref. Na soisk. Uch. step. Kand. polit. Nauk. – M., 2009. – S. 25.

2 V. Pashkov. Informacionnaja bezopasnost’ SShA // Zarubezhnoe voennoe obozrenie №10 2010. – S. 3-13.

3 Gracheva V.T. Osnovy mogushhestva SShA // http://www.km.ru/referats/E5DD6DA3EF3543C3B1ADA9967F350E01

4 Rogovskij E.A. SShA: informacionnoe obshhestvo (jekonomika i politika). Izdatel’stvo: Mezhdunarodnye otnoshenija, 2012. – 408 s.

5 Shherbakova T.V. Kommunikacionnyj menedzhment vo vneshnej politike SShA v konce XX veka. Avtoref. Na soisk. Uch. step. Kand. istor. Nauk. – M., 2006. – S. 25.

6 A. Sagageljan. K voprosu o problemnyh aspektah informacionnoj politiki gosudarstva // Problemnye aspekty gosudarstvennoj informacionnoj politiki stran perehodnogo perioda. Materialy Vserossijskoj nauchno-prakticheskoj konferencii. -- Kirov, 2010. – T. II. – S. 181.

7 Komleva N.A. Kollektivnaja bezopasnost’ na sovremennom jetape // [Jelektronnyj resurs]. – Rezhim dostupa: http://www.roman.by/r-89725.html.

8 Hohlysheva O.O. Vseob#emljushhaja bezopasnost’ i ee mezhdunarodno-pravovoe obespechenie v uslovijah globalizacii // Vestnik Nizhegorodskogo universiteta im. N.I. Lobachevskogo. 2012. – № 3(1). – S. 323-331.

9 Glotova S.V. Direktivy Evropejskogo Soobshhestva: avtoref. dis. … k.ju.n.: 12.00.10. – M., 1999. – S. 25.

10 Evropejskij Sojuz: osnovopolagajushhie akty v redakcii Lissabonskogo dogovora s kommentarijami / otv. red. S.Ju. Kashkin. – M., 2010. – S. 554-570.

11 Fedorov A.V. Informacionnaja bezopasnost’ v mirovom politicheskom processe. – M., 2006. – S. 183.