КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ
ИМЕНИ АЛЬ-ФАРАБИ

УНИВЕРСИТЕТ «ТУРАН»

ПРАВОВЫЕ ОСНОВЫ БОРЬБЫ С ПРАВОНАРУШЕНИЯМИ В ГЛОБАЛЬНЫХ КОММУНИКАЦИОННЫХ СЕТЯХ

Сборник материалов международной научно-практической конференции (8 октября 2014 года)

Алматы 2014

***

In this article were researched the normative and legal acts in the field of the struggle with the crimes in the global communication net through the supplement of the national security of the state. The analysis of the national security in the Republic of Kazakhstan and its aspects was given.

***

Бұл мақалада құқықтық нормативтік заңдар ұлттық қауыпсіздік туралы карастырылады. Қазіргі ұлттық қауыпсіздіктіңерекшеліктері талдау жасалған, оның өзгерістерінің мен бағыттары көрсетілген.

К вопросу о нормативно-правовой основе обеспечения информационной безопасности на примере США

Губайдуллина М.Ш.,
профессор кафедры международных отношений
и мировой экономики КазНУ им. аль-Фараби,
директор Центра германских исследований

Противоречие глобализации: между принципом свободы доступа к информации и правом безопасности информации

Глобальное информационное сообщество основывается на общем для всех стран технологическом фундаменте, на развитии информационно-коммуникационной инфраструктуры. Конкуренция и противоречия противоборствующих сторон принимают различные формы, протекают с различной степенью интенсивности и конфликтности, иногда дело доходит до открытых конфликтов в информационном пространстве, информационных войн. Современные процессы политической жизни, международных отношений происходят в так называемой транспарентной зоне, находятся в режиме относительно легкого доступа. Они изначально прозр-

для ее «эксплуатации» СМИ, сторонними акторами (обсуждение в соцсетях, отклики, трактовки, намеренное искажение и введение в заблуждение и т.д.). Речь идет об информационных войнах, когда наиболее «качественная» информация или наоборот умело сфабрикованная становится сильным оружием в борьбе с предполагаемым противником, для чего используется сеть Интернет с ее безграничными возможностями.

Итак, появление и ежегодное совершенствование технологий и Интернета сопровождается множеством проблем в киберпространстве. Основная проблема заключается в ухудшении ситуации с информационной безопасностью. Огромный рост числа локальных сетей и пользователей Интернета рождает немало авантюристов, хулиганов и преступников, что стимулирует поиск новых методов борьбы с взломщиками (хакерами) информационных ресурсов.

Соединенные Штаты с их продвинутыми высокими технологиями, где традиционно государственная мощь опирается на технический прогресс, одновременно стремятся выступать гарантами по обеспечению правовой защиты новейших технологий. Лидирующая позиция США определяется сильными позициями в производстве компьютеров и программного обеспечения, уровнем распространения сетей. Политика приоритетного формирования технологической инфраструктуры обеспечивает стимулирование высокорисковых, но перспективных технологий, которые будут способствовать созданию принципиально новых продуктов и услуг, а также продвижению их на мировые рынки. Такая политика «двойных технологий», являясь частью государственной программы технологической безопасности США, существенно стимулирует процесс сближения гражданской и военной промышленности. Эта политика также направлена на развитие законодательства по обеспечению информационной безопасности, которое насчитывает сегодня до 500 законодательных актов.

Первые шаги по законодательному обеспечению информационной безопасности

В середине 80-х годов прошлого столетия информационная безопасность (ИБ) Соединенных Штатов рассматривалась с точ-

ничена информационной системой с автономными и локальными ресурсами. При этом ИБ была сконцентрирована на триединстве запретительных мер или трёх «НЕ»: (1) не допустить; (2) не пропустить; (3) не упустить. Защита информационных ресурсов, направленная на выполнение главных задач ИБ, состояла в том, чтобы ограничить круг пользователей; создать доступ в системы по паролям; разграничить информацию по категориям. Для этого требовалась современная правовая защита и законодательная основа.

Считается, что первый в мировой практике закон об информационной безопасности – это «Закон о компьютерной безопасности» [1] был принят в Соединенных Штатах в 1987 г., то есть практически одновременно с рождением эры Интернета. Это был законодательный акт по обеспечению безопасности информации в федеральных компьютерных системах. Он включал правовую ответственность за умышленное проникновение, порчу информационных ресурсов, их использование в преступных целях. Непосредственным исполнителем закона назван Национальный институт стандартов и технологий (НИСТ), отвечающий за выпуск стандартов и руководств, направленных на защиту от уничтожения и несанкционированного доступа к информации, а также от краж и *подлогов*, выполняемых с помощью компьютеров.

Соединенные Штаты, где сформировано общество массового потребления, стали страной, которая непосредственно оказалась в ловушке собственных достижений и своего технологического скачка. Персональные компьютеры с сетевыми операционными системами сравнительно быстро вошли жизнь западного общества, стали предметом первой необходимости на производстве, на рабочем месте любого клерка, в домашнем употреблении.

Одна из крупнейших ТНК по производству программного обеспечения для различного рода вычислительной техники (ПК, игровых приставок, мобильных телефонов и прочего) является Корпорация Microsoft. Она была основана в 1975 г. студентами Гарвардского университета Биллом Гейтсом и Полом Алленом. Американская мечта Билла Гейтса, главной фигуры компании Microsoft заключалась в том, чтобы «компьютер появился на каждом столе и в каждом доме», очень скоро стала реальностью.

Microsoft и его продукция (операционные системы типа Windows, MS Office, Word, Excel, Outlook, Power Point, Internet Explorer и др., приложения типа Word и Excel) сегодня доминируют на рынке новейших достижений. Главным фактором роста Microsoft называют ее стратегию развития, обеспечивающую компании очень сильных и высококвалифицированных сотрудников. Своим работникам Гейтс выплачивает вознаграждения в виде акции, с помощью которых он сделал миллионерами большинство людей.

В США Microsoft финансирует несколько государственных политических институтов, в частности American Enterprise Institute, Cato Institute, Центр стратегических и международных исследований и фонд «Наследия». В различных странах действует программа Microsoft Software Donation, направленная на бесплатное предоставление программного обеспечения неправительственным организациям [2].

Со стороны американского правительства была оказана всевозможная поддержка для развития информационной инфраструктуры, а также принят ряд законов для распространения компьютеризации. Производство компьютеров, направленное на широкого потребителя, было изначально поставлено на массовую основу. Американские компании составляют большую часть информационно-коммуникационной инфраструктуры по всему миру (60% информационного бизнеса принадлежит США). Естественно, что новейшие свои разработки они пускают для испытания на рынки потребления Соединенных Штатов и большинства стран мира, так как именно американское общество на сегодняшний день наиболее продвинуто в сфере использования информационных технологий и средств коммуникации.

В свою очередь, «массовизация» потребления в компьютерной сфере привела также и к другим, более серьезным последствиям. Известны десятки и сотни скандальных историй о крупных мошенничествах в банковской и финансовой сфере, миллиардные убытки от «электронного» воровства и компьютерных вирусов, множество утечек сведений из секретных документов, посвященных политическим вопросам, ведения информационной войны в один момент стали представлять серьезнейшую опасность для национальной безопасности США.

Уже в 1995 г. в СМИ заговорили о проблеме информационной безопасности, затем появились первые публикации, в которых такая проблема обосновывалась как концепция информационного противоборства и информационной войны [3]. В 1998 г. президент Б. Клинтон принял директиву PDD-63, а в январе 2000 г. – «Национальный план защиты информационных систем на 2000-2003 гг.» как «всеобъемлющее видение задач по защите ключевых секторов экономики, национальной безопасности, общественного здравоохранения и личной безопасности граждан». В этих документах информационная безопасность напрямую связывалась с безопасностью инфраструктуры страны и благополучием американской нации. В соответствии с этими документами были созданы Совет по безопасности национальной инфраструктуры (NIAC) и специальные центры компьютерной и информационной безопасности: в Пентагоне — Объединенный центр защиты сетей (JTF-CND), в ФБР — Национальный центр защиты инфраструктуры (NIPC), а также Национальный и Федеральный центры реагирования на компьютерные происшествия (NSIRC, FedCIRC). Все они с помощью специальной федеральной сети обнаружения вторжения (FIDNet) должны оповещать правительственные, промышленные, коммерческие и общественные организации об угрозе информационного нападения на США [4]. Это были первые шаги федерального правительства решить проблему обеспечения информационной безопасности современного американского общества.

К началу 2000-х годов основными угрозами информационной безопасности признаны несанкционированные проникновения через Интернет в информационные ресурсы страны, к распределенным базам данных на основе технологии клиент-сервер. Данные свидетельствовали об увеличении на 10% числа случаев, подвергшихся влиянию программ-вирусов, на 2% увеличилось количество отказов в обслуживании, связанных с переполнением буфера при спамах в электронной почте и т.д. [5].

Согласно первому закону и всем последующим, операторы федеральных информационных систем, что содержали конфиденциальную информацию, должны обладать собственной системой обеспечения ИБ, куда включен также профессионально

обученный персонал. Технологический прогресс особенно стал ощутим вместе с появлением операционных систем с многоуровневой защитой от несанкционированного доступа. Появились новые методы криптографии для шифрования транзакций, широко внедрялись интеллектуальные аппараты и средства блокирования подключения устройств. Так, смарт-карты явились технологическим ноу-хау, ведь пластиковые карты со встроенной микросхемой содержали микропроцессор и операционную систему, контролирующую устройство и доступ к объектам в его памяти.

Учитывая необходимость защиты конфиденциальной информации, на Национальный институт стандартов и технологий США (НИСТ) была возложена ответственность за оперативное введение стандартов и руководств по защите от уничтожения и несанкционированного проникновения к информации, в сферу деятельности института входит также серьезный анализ масштабов уязвимых мест, определение их природы. НИСТ получил право вводить нормативы по защите от краж и подлогов, производимых с помощью компьютеров, которые имеют законодательное обеспечение. Так, в 1997 г. появился законопроект «О совершенствовании информационной безопасности» (Computer Security Enhancement Act of 1997, H.R. 1903), направленный на усиление роли НИСТ и упрощение операций с криптосредствами. Законопроект констатировал, что частный сектор должен предоставлять криптосредства для обеспечения конфиденциальности и целостности данных (в том числе аутентичности), что разработка и использование шифровальных технологий должны происходить на основании требований рынка, а не распоряжений правительства.

Важно, что нормативы и законодательство направлены на обеспечение национальной безопасности в информационной сфере, включая госструктуры (Министерство обороны, Министерство энергетики, Агентство национальной безопасности (АНБ) и др.). Согласно разделу 6 Закона, все правительственные ведомства обязаны иметь план обеспечения информационной безопасности, направленный на то, чтобы компенсировать риски и предотвратить возможный ущерб от утери, неправильного использования, несанкционированного доступа или модификации информации в федеральных системах.

Итак, законотворческая деятельность в США не отстает от прогресса информационных технологий.

Информационная безопасность в условиях борьбы с международным терроризмом: законодательные и институциональные изменения

Опасность со стороны международного терроризма после терактов 11 сентября 2001 г. заставила правительство США усилить всю инфраструктуру безопасности, включая информационную сферу. Была реорганизована вся система национальной безопасности США, принят закон о борьбе с терроризмом – «Акт 2001 года, сплачивающий и укрепляющий Америку обеспечением надлежащими орудиями, требуемыми для пресечения терроризма и воспрепятствования ему», который получил название «Акт патриота США 2001 года» [6]. Этот федеральный закон дает правительству и полиции широкие полномочия по надзору за гражданами, расширил права ФБР по подслушиванию и электронной слежке, что многими было расценено как нарушение четвертой поправки к Конституции США. Срок действия настоящего Закона несколько раз продлевали, так как он широко охватывает важнейшие сферы безопасности государства и граждан, в том числе в сфере информационной деятельности и безоапасности: полномочия президента и членов кабинета; деятельность и полномочия правоохранительных органов; разведка и контрразведка; банковская и финансовая деятельность; наркобизнес; и отмывание денег; охрана границ и вопросы иммиграционного контроля; валютный контроль; контроль за иностранными учащимися; деятельность министерства юстиции и полномочия судов; процессуальный режим расследования и оперативной работы; порядок проведения оперативных мероприятий (прослушивание, электронное наблюдение, отслеживание и регистрация телефонных звонков); проведение негласных обысков и осмотров помещений; межведомственная координация правоохранительных и разведывательных органов; помощь пострадавшим или семьям пострадавших от актов терроризма; информационная безопасность; вопросы борьбы с киберпреступностью и биотерроризмом.

Итак, закон допускает применение различных видов электронного наблюдения, формы «обыска и изъятия». Закон допускает выдачу судебного ордера на «кочующее» прослушивание телефонных разговоров с помощью электронных средств, то есть в отношении разговоров объекта наблюдения со всех телефонных аппаратов при его передвижении. Закон уполномочивает судью выдавать ордера на использование определителей телефонных номеров сообщающихся абонентов «в любом месте Соединенных Штатов», а не только в пределах территориальной юрисдикции суда. Закон обязывал провайдеров сети предоставлять правоохранительным органам электронные сообщения лиц, подозреваемых в терроризме.

Таким образом, США стали первой страной, которая допустила введения в законодательном порядке электронного наблюдения, если того требовала необходимость уголовного розыска, контрразведывательные операции и некоторые другие случаи. Правоохранительные органы на федеральном уровне получили право вести розыск подозреваемых в терроризме личностей оперативным наблюдением за Интернетом. ФБР разработало систему онлайн–наблюдения «Carnivore» [7], отслеживание посещений Web-страниц и корреспондентов по электронной переписке, в некоторых случаях, при наличии чрезвычайных обстоятельств – без ордера, выдаваемого судом, лишь с одобрения прокуратуры. Был разрешен режим получения санкции на отслеживание телефонных номеров при обмене сообщениями по электронной почте и посещения сайтов в Интернете.

6 февраля 2002 г. президент Буш обратился к Конгрессу США с новым законопроектом о бюджете страны на период 2003-2007 гг. [8]. В ряду государственных расходов четко просматривается тенденция на увеличение бюджетных ассигнований в области национальной безопасности. Только на развитие информационных технологий предполагалось выделить свыше 290 млрд. долл., почти в два раза больше, чем за предыдущие пять лет или примерно весь бюджет Пентагона за 2001 г.

Тогда же были произведены институциональные преобразования, направленные на укрепление национальной безопасности. В 2002 г. были созданы Управление внутренней безопасности;

Совет внутренней безопасности (СВБ) и Министерство внутренней безопасности для противодействия угрозам терроризма и экстремизма. Исполнение конкретных задач возлагалось на пять департаментов данного министерства: (1) Департамент анализа информации и защита стратегически важных объектов инфраструктуры; (2) Департамент по противодействию теракту с применением химического, биологического и ядерного оружия; (3) Департамент по обеспечению безопасности государственных границ и перевозок; (4) Департамент по обеспечению готовности к действиям уполномоченных структур в чрезвычайных ситуациях; (5) Департамент по координации с др. федеральными министерствами, правительствами штатов, местными органами власти, с частным сектором.

Так, Департамент анализа информации и защиты стратегически важных объектов инфраструктуры среди прочего должен обеспечивать: получение и анализ всех видов информации с целью определения природы и масштабов потенциальной террористической угрозы; экспертные оценки степени уязвимости ключевых ресурсов и инфраструктуры; формирование национальной стратегии по охране ключевых ресурсов и инфраструктуры; предоставление предупреждающей информации федеральным и местным органам власти и частному сектору, и др.

Следующие задачи определяют деятельность Департамента анализа информации и защиты инфраструктуры, создавая структурную сеть: центр защиты национальной инфраструктуры ФБР; система национальных коммуникаций Министерства обороны; управление страхования ключевой инфраструктуры Министерства торговли; отдел компьютерной безопасности Национального института стандартов и технологий; центр моделирования и анализа национальной инфраструктуры Министерства энергетики и др.

В целом, Министерство внутренней безопасности состоит из 22 различных управлений, в которых занято около 170 тыс. сотрудников, а бюджет составляет порядка 37 млрд. долл. в год [9]. Программа безопасности, предусматривающая экономически оправданные защитные меры и синхронизированная с жизненным циклом ИС, упоминается в законодательстве США неоднократно. Согласно пункту 3534 («Обязанности федеральных ведомств»)

подглавы II («*Информационная* [illegible]») главы 35 («*Координация* федеральной информационной политики») рубрики 44 («Общественные издания и документы»).

Таким образом, угроза международного терроризма стимулировала развитие новых подходов к борьбе с угрозами и преступлениями в сфере информационной безопасности.

Кибертерроризм

Законом в соответствии с «Актом патриота США 2001 года» введены в оборот некоторые новые понятия, расширяющие трактовку термина «терроризм», которые прежде содержались в действующем федеральном законодательстве, было расширено понятие «федеральное преступление, связанное с терроризмом».

В законе присутствует новое понятие «кибертерроризм», под которым понимается ряд преступных действий, включающих различные квалифицированные формы хакерства, нанесение ущерба защищенным компьютерным сетям граждан, юридических лиц и государственных ведомств. Этот ряд продолжен перечислением ущерба медицинскому оборудованию, также «физический вред какому-либо лицу», «угрозу общественному здоровью или безопасности», «ущерб, причиненный компьютерной системе, используемой государственным учреждением при отправлении правосудия, организации национальной обороны или обеспечении национальной безопасности» [10].

Понятие «кибертерроризм» включает уголовно наказуемые деяния, хакерские посягательства, наносящие материальный ущерб на совокупную сумму от 5000 долл. и выше, и наказываемые крупными штрафами или наказанием в виде лишения свободы от пяти до двадцати лет. Были расширены возможности различных форм электронного наблюдения.

Каждый компьютер сети и вычислительное устройство, предназначенный для передачи информации через Интернет, должен иметь уникальный адрес, чтобы отправлять и получать сообщения. Интернет-корпорация по присвоению имен и номеров (ICANN) отвечает за задачи управления Интернет-адресами, которые образуют систему адресации Internet Protocol (IP), в которую входит каждое уникальное интернет-устройство с единст-

венным IP (компьютер, сотовый телефон, персональный цифровой устройство). В этой связи сведения о регистрации IP или WHOIS данные на владельцев Интернет-адресов представляют источник раздора между безопасностью/свободой слова/защитой прав человека/правопорядком/коммерческими и государственными интересами.

Американское правительство продолжает законотворческую деятельность в сфере информационной безопасности. 12 февраля 2013 г. президент США Барак Обама подписал закон, разрешающий федеральным управлениям предоставлять частным компаниям информацию о киберугрозах, в целях снижения риска взлома критической инфраструктуры [11]. В этой связи правительственные организации США будут обязаны предоставлять частным компаниям информацию о киберугрозах. Говорится, что инциденты безопасности могут иметь катастрофические последствия для здоровья граждан, а также для общественной, экономической и национальной безопасности. Для некоторых компаний, задействованных в критической инфраструктуре, обмен данным будет проходить на добровольной основе, тогда как правительственные организации обязаны проводить надзор над критической инфраструктурой для идентификации операторов и отраслей, наиболее подверженных риску, и требовать от них принятия мер безопасности. Закон обязывает министров внутренней безопасности, обороны и юстиции, а также главу национальной разведки предоставлять критическую информацию частным компаниям США.

Работа над созданием систем безопасности для операторов критической инфраструктуры возложена на Национальный институт стандартов и технологий США. Конгрессмен Майкл Маккол (Michael McCaul) выразил обеспокоенность тем, что указ потребует принятия дополнительных инструкций и предписаний для американских бизнесменов, поскольку указ приведет к появлению новых регуляторов, которые будут «тормозить» нововведения и усложнят ведение бизнеса. Наоборот, национальная организация American Civil Liberties Union одобрила указ Обамы, отметив, что данный документ позволит лучше защитить конфиденциальные данные, чем Cyber Intelligence Sharing and Protection Act (CISPA).

Возможно, указ Барака Обамы, повторяет указ предыдущего президента за N13231, специально посвященный вопросам информационной безопасности страны – «Защита критической инфраструктуры в информационный век». В соответствии с ним был создан Комитет при президенте по вопросам защиты критической инфраструктуры во главе с председателем Ричардом Кларком, выполняющим одновременно функции специального советника президента по вопросам безопасности кибернетического пространства. Основная функция комитета заключалась в координации всех федеральных программ в области информационной безопасности независимо от их ведомственной принадлежности. При этом на Бюджетное управление при президенте (Office of Management and Budget) был возложен жесткий контроль за эффективностью использования ассигнований, выделяемых Конгрессом на программы в области развития информационных технологий (ИТ) и обеспечения информационной безопасности (ИБ) всех министерств и ведомств США. Последнее обстоятельство выводит вопросы информационной безопасности на первое место среди приоритетных направлений совершенствования всей системы национальной безопасности США.

Заключение

В современном мире глобальных сетей ни одно государство не имеет средств для абсолютной защиты информационной безопасности. Интернет и социальные сети становятся средством достижения военных и политических целей, следовательно, угрозам подвержена национальная безопасность.

В этой связи законодательный уровень нуждается в разработке общемировых стандартов и приведения в соответствия с ними национальные законодательства, то есть нормативно-правовая база любого государства должна быть согласована с международной практикой. При этом остается проблема, которая заключается в том, как разработать новые законы с учетом интересов всех категорий субъектов информационных отношений; как обеспечить баланс созидательных и ограничительных (преследующих цель наказать виновных) законов и др.

Интегрируя в международное правовое пространство, Казахстанские стандарты и сертификационные нормативы не должны

отставать от темпов и уровня мирового развития информационных технологий, соответственно, они должны мобильно реагировать на любые изменения в данной сфере, должны обеспечивать информационную безопасность.

Литература:

1. Computer Security Act of 1987 // Public Law 100-235 (H.R. 145), January 8, 1988
2. Сайт компании Microsoft: <http://www.microsoft.com/About/ Corporate Citizenship/CommunityInvestment/NGO/ru/softwaveGrants.mspx>
3. Libici, Martin. What is Information Warfare. – National Defense University. – ACIS paper 3, August 1995: IWS (The Information Warfare Site): <http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003cont.html>
4. Леваков А. Анатомия информационной безопасности // Jet Info. Информационный бюллетень. – 2002. – № 6 (109). – С. 5.
5. Внешние утрозы ИБ: < http://www.freelance.narod.ru/IS_USA.html>
6. USA Patriot Act (107th Congress, 1st Session, In the Senate of the United States, October 24, 2001, H.R. 3162 RDS) (Акт патриота США 2001 г.)/ «Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001» (Акт о сплочении и укреплении Америки путем обеспечения надлежащими средствами, требуемыми для пресечения и воспрепятствования терроризму, 2001 г.): Electronic Privacy Information Center Site (EPIC): <http://www.epic.org/privacy/terrorism/hr3162.html>
7. Carnivore (программное обеспечение) — система разведки
8. Performance Information for Major IT Investments, February 4 2002, President's Budget for 2003, cross-reference Chapter 22 of the Analytical Perspectives Section, of the 2003 Budget. Page 1 of 89
9. Селиванова В. Реформа системы внутренней безопасности США // США – Канада. Экономика – политика – культура. – 2003. – № 1. – С. 82–84
10. См.: USA Patriot Act, 2001
11. The Information Technology Security Evaluation Criteria (ITSEC): <http://www.itsec.ru/newstext.php?news_id=90154#sthash.jYPeei9W.dpuf>, 13.02.2013

On the question of the regulatory framework to ensure data security system on the example of the United States

***

In the era of globalization and ubiquitous informational formed a new medium – cyberspace, where the face of political, economic and commercial interests, the business environment, and so on, leaving the level of inter-state and transnational relations. Of considerable importance is the policy of the United States to maintain a high level of technological progress and the development of the information society.