Р. М. Асланов

ЗАРУБЕЖНЫЙ ОПЫТ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: В основных нормативных документах США и в законодательстве европейских государств информационная и сетевая безопасность понимается как способность сети или системы противостоять с данным уровнем надежности авариям или злонамеренным действиям, могущим нарушить доступность, целостность и конфиденциальность хранимой или передаваемой информации, а также услуг, предоставляемых посредством сети или информационной системы. Соблюдение безопасности определяется как доступность, идентификация, целостность, конфиденциальность информации. Особое внимание при этом уделяется законодательной базе, затрагивающей вопросы перехвата и дешифровки информации.
Ключевые слова: юриспруденция, регулирование, информация, безопасность, система, доступность, целостность, конфиденциальность, идентификация, легальность.

В основных нормативных документах США и в законодательстве европейских государств информационная и сетевая безопасность понимается как способность сети или системы противостоять с данным уровнем надежности авариям или злонамеренным действиям, могущим нарушить доступность, целостность и конфиденциальность хранимой или передаваемой информации, а также услуг, предоставляемых посредством сети или информационной системы. Соблюдение безопасности определяется как доступность, идентификация, целостность, конфиденциальность информации. Особое внимание при этом уделяется законодательной базе, затрагивающей вопросы перехвата и дешифровки информации.

Так, в Законе США «Об управлении информационной безопасностью» 2002 года информационная безопасность определяется как[1]:

- защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, распространения, модификации или уничтожения;
- обеспечение целостности информации от неправомерного изменения или уничтожения, включая гарантии ее подлинности;
- обеспечение конфиденциальности, означающей поддержание установленных ограничений доступа и распространения информации, включая закрытость данных о частной жизни и о собственности;
- доступность, означающую быстрый и надежный доступ к информации.

Для многих зарубежных государств в основном характерен подход к проблеме информационной безопасности с учетом таких понятий, как «аутентичность», «доступность», «целостность», «конфиденциальность».

Так, в Болгарии действует Закон о секретной информации от 2002 года, который ограничивает право широкой общественности на доступ к информации, давая возможность любому чиновнику присвоить любому документу гриф секретности.

Закон США 1998 года о защите информации приводит аналогичный закон 1984 года в соответствие с требованиями Директивы Европейского Союза о защите информации и, распространяет его на учетные записи, ведущиеся государственными учреждениями и частными компаниями, устанавливает ряд ограничений на использование персональных данных и на доступ к учетным записям, а также обязывает юридических лиц, ведущих такие записи, регистрироваться в Комиссариате по защите информации, который является независимым агентством, обеспечивающим соблюдение требований закона.

Положения о неприкосновенности частной жизни содержатся и в ряде других законодательных актов, например в законах, регламентирующих ведение медицинских записей и хранение информации о потребительских кредитах, а также в законах: «О реабилитации правонарушителей» (1974 г.), «О телекоммуникациях» (1984 г.), «О полиции» (1997 г.); Раздел VI «Закона о вещании» (1996 г.) и «Закон о защите от преследова-

[1] The Federal Information Security Management Act of 2002 (“FISMA”, 44 U.S.C. § 3541, et seq.

ний» (1997 г.). Некоторые положения перечисленных законов были изменены в связи с принятием Закона о защите информации в редакции 1998 года.

Принятый в 1985 году Закон США о перехвате коммуникационных сообщений[2] устанавливает ряд ограничений по контролю над телекоммуникационными средствами. В июне 1999 года были изданы рекомендации по установке подслушивающих устройств, требующие внесения многочисленных поправок в указанные законы, в частности, в сфере обеспечения содействия установке подслушивающих устройств со стороны провайдеров Интернет-услуг; продления срока действия таких устройств до трех месяцев; разрешения на использование подслушивающих устройств с возможностями роуминга. Но такие важные проблемы, как контроль со стороны судебных органов и государственный надзор за перехватами информации, в указанных рекомендациях не затрагиваются.

Как показывает анализ зарубежного опыта правового обеспечения информационной безопасности около 100 государств приняли законы о праве на информацию[3].

Устойчивая тенденция на принятие национальных законов, гарантирующих доступ к информации о деятельности органов власти, отмечается с начала 60-х гг.

В последние 20 лет такие законы были приняты во Франции, Греции, Дании, Голландии, Бельгии, Португалии, Испании, Финляндии и Италии.

Законы о доступе граждан к правительственной информации приняты в США, Канаде, Австралии и Новой Зеландии.

В ряде стран Европы, таких как Нидерланды, Испания, Португалия, Австрия, Венгрия, Эстония, Бельгия и Румыния, право граждан на доступ к официальной информации закреплено конституционно. Во Франции, Греции и Италии – эти права закреплены в законах. Совершенствование законодательства в данной сфере продолжается в Великобритании, Германии, Эстонии, Молдове, Польше и ряде других государств.

Законодательное ограничение прав на доступ к правительственной информации установлено, например, в Швеции и Финляндии.

В рамках данной работы представляется особенно важным отметить, что в настоящее время во многих государствах разрабатываются и реализуются концепции электронного правительства, основывающиеся на применении информационных технологий при создании государственных информационных ресурсов и доступе к информации о деятельности государственных органов власти (США, Сингапур, Австралия, Новая Зеландия и другие).

В Великобритании Акт о свободе информации 2000 года предусматривает, что основной целью действия системы правительственной информации является обеспечение доступа к большому массиву официальных данных обеспечивает право граждан на доступ к правительственной информации по первому требованию.

Следует отметить, что правовая база для создания системы правительственной информации в Великобритании, например, содержится в Своде правил по доступу к правительственной информации и основана на бесплатном предоставлении населению услуг по обеспечению их информационных потребностей и реализации прав и обязанностей.

В Австрии также законодательно закреплено право граждан на доступ к нормативной правовой базе, при этом информация, находящаяся в распоряжении государственного сектора, не коммерциализирована, а большой массив информации предоставляется по более низким ценам, и плата за указанные информационные услуги взимается за копирование и распространение.

На электронные документы также распространяется действие Закона о свободе информации Дании, который представляет гражданам равное право доступа к правительственным документам, и распространением информации о деятельности государственных органов в основном занимается государство, которое, учитывая коммерческий интерес к информации, осуществляет сотрудничество с негосударственными структурами.

Аналогичные положения содержатся в Законе Финляндии об открытости официальных документов.

Во Франции такие правовые нормы закреплены в Законе о взаимодействии государственной администрации и общества, которым запрещена перепечатка, распространение и коммерческое использование полученных документов, а ознакомление с документами является бесплатной услугой (плата взимается только за копирование). Циркуляром премьер-министра 1994 года о распространении правительственной информа-

[2] The Interception of Communications Act (IOCA) (1985)

[3] И. Дзялошинский «Российский и зарубежный опыт правового регулирования доступа граждан к правительственной информации» - М. 1999.

ции установлены некоторые принципы коммерциализации этой информации, связанные с предоставлением необработанной информации на безвозмездной основе и данных защищенных авторским правом, распространяемых за определенную плату.

В Германии доступ к отдельным видам информации регламентирован отраслевым законодательством и пока не приняты общие законы.

В Португалии Закон о доступе к информации государственного сектора регламентирует распространение правительственной информации через систему «специализированных киосков», техническое оснащение которых возложено на частный сектор.

В то же время сфера действия Закона Испании «О доступе к информации» не распространяется на электронную информацию, а вопросы электронного обмена документами регламентированы Законом «Об услугах информационного общества и электронной торговле», принятым в 2002 году.

Анализ зарубежного опыта правового регулирования вопросов доступа к информации свидетельствует не только об общих тенденциях, но и о различных подходах.

Значительный массив законодательных и иных нормативных правовых актов в области обеспечения информационной безопасности во многих зарубежных государствах касается электронной торговли и использования электронных подписей: Закон Канады «Об электронных сделках» 1999 года, Федеральный закон США «Об электронных подписях в международной и внутренней торговле» 2000 года, Закон Ирландии «Об электронной торговле» 2000 года, Закон Испании «Об услугах информационного общества и электронной торговле» 2002 года, Закон Южной Кореи «Об электронной торговле» 2001 года, «Ордонанс об электронных сделках» Гонконга 2000 года, Закон Таиланда «Об электронных сделках и электронной подписи» 2002 года. В 2002 году приняты законодательные акты об электронных сделках в Турции и Пакистане.

В Законе Германии «О телекоммуникациях»[4] 1996 года предоставление телекоммуникационных услуг населению независимо от места жительства и за доступную плату отнесено к универсальным услугам в информационной сфере общественных отношений.

Анализ показывает, что нормативные правовые акты, регулирующие защиту информации, информационной техники и технологий, направленные на создание и защиту информационных сетей, устанавливающие единые условия использования линий связи и коммуникационных услуг, действуют уже в целом ряде государств.

Что касается коммерческой информации, то такие законодательные акты приняты в Великобритании, Франции, США, Канаде и многих других[5].

Особого внимания в области правового обеспечения информационной безопасности заслуживают вопросы защиты персональных данных, регламентированные во многих государствах.

Одной из актуальнейших в настоящее время во всем мире является проблема правового регулирования в Интернете.

Всемирная информационно-телекоммуникационная сеть Интернет наряду с объективными благами, которые она дает человечеству, впитала в себя, к сожалению, и многие пороки общества, создающие и новые формы (виды) преступной деятельности и принципиально новые угрозы, не совместимые с задачами поддержания мировой стабильности и безопасности.

В ряде европейских государств, например во Франции, приняты законы, в которых предусмотрена обязательная регистрация всех владельцев веб-сайтов и обязанность провайдеров сообщать сведения об авторах сайтов любому заинтересованному третьему лицу, при этом запрещается предоставление «хостинга» неидентифицированным пользователям. За нарушение этих норм установлена уголовная ответственность провайдеров. Также предусматривается уголовная ответственность и авторов сайтов за предоставление неполных или недостоверных личных данных. Введена проверка на уровне провайдера, а все Интернет-сайты, авторство которых не установлено, переходят под ответственность провайдера. В рамках законов по борьбе с организованной преступностью и с особо опасными преступлениями предусматривается наказание в виде лишения свободы за распространение любыми техническими средствами информации, позволяющей изготавливать технические устройства.

В Великобритании фильтрация контента (содержания) Интернет-ресурсов осуществляется Национальным отделением по борьбе с преступлениями в сфере высоких технологий. Существует также «горячая линия» по разбору жалоб по этим вопросам – «Фонд Интернет – Наблюдения». Провайдер обязан

[4] Telekommunikationsgesetz (TKG)

[5] Рачковский В.В. «Зарубежное законодательство о коммерческой тайне» - Правоведение. – 1999. - №3

после получения информации о противоправности содержания немедленно удалить материал с сервера, в этом случае провайдер не подвергается преследованию. Аналогичный опыт имеется в Германии и ряде других стран.

Так, в Канаде законы 1997 г. о позитивном доступе в Интернет и о сохранении конфиденциальности в Интернете федеральными структурами направлены на защиту пользователей сети Интернет, в том числе на обеспечение конфиденциальности информации о них самих.

«Закон о защите детей от «хищников» в Интернете» 1997г. и «Закон о правах потребителя в электронной торговле» 1997г. регламентируют правила изготовления и распространения коммерческой рекламы, ориентированной на массового потребителя[6].

В США в соответствии с «Законом об электронном государстве» 2002г. под информационной безопасностью понимается защита информации и информационных систем от неразрешенного доступа, использования, раскрытия, распространения, модификации или уничтожения, обеспечение неприкосновенности, конфиденциальности.

Ключевую роль в области обеспечения информационной безопасности также играет американский «Закон об информационной безопасности»[7]. Его цель – реализация минимально достаточных действий по обеспечению безопасности информации в федеральных компьютерных системах, без ограничений всего спектра возможных действий.

Таким образом, анализ показывает, что понятие и содержание информационной безопасности в США прошло известную эволюцию от обеспечения идеи «свободной личности» – с одной стороны, и до «максимального учета национальной безопасности» – с другой.

Библиография:

1. И. Дзялошинский «Российский и зарубежный опыт правового регулирования доступа граждан к правительственной информации» - М. 1999.
2. Коровин Д.В. «Правовые аспекты деятельности Интернета» // США, Канада: экономика, политика, культура. 2001. №8
3. Рачковский В.В. «Зарубежное законодательство о коммерческой тайне» - Правоведение. – 1999. - №3
4. Computer Security Act of 1987, Public Law 100-235 (H.R. 145), January 8, 1988
5. Telekommunikationsgesetz (TKG)
6. The Interception of Communications Act (IOCA) (1985)

References (transliteration):

1. I. Dzjaloshinskij «Rossijskij i zarubezhnyj opyt pravovogo regulirovanija dostupa grazhdan k pravitel’stvennoj informacii» - M. 1999.
2. Korovin D.V. «Pravovye aspekty dejatel’nosti Interneta» // SShA, Kanada: jekonomika, politika, kul’tura. 2001. №8
3. Rachkovskij V.V. «Zarubezhnoe zakonodatel’stvo o kommercheskoj tajne» - Pravovedenie. – 1999. - №3
4. Computer Security Act of 1987, Public Law 100-235 (H.R. 145), January 8, 1988
5. Telekommunikationsgesetz (TKG)
6. The Interception of Communications Act (IOCA) (1985)

[6] Коровин, Д.В. «Правовые аспекты деятельности Интернета» // США, Канада: экономика, политика, культура. 2001. №8

[7] Computer Security Act of 1987, Public Law 100-235 (H.R. 145), January 8, 1988