

этого количества ресурсов следует исключить 3 туристических портала, которые не являются собственностью конкретной туристической компании. Анализ качества оставшегося количества ресурсов позволяет сделать следующие выводы:

- 30 % ресурсов не представляют интереса для пользователей, так и не работают на компанию их создавшую в силу того, что эти сайты не обновлялись и были сделаны очень давно;

- 20 % – «сайты ради галочки» – ситуация, когда сайт был сделан, несколько раз в пики сезонов обновлен, но ничего не делается для его продвижения на рынке;

- 40 % – «средний класс» – сайты отвечают большинству потребностей посетителя: информация о компании, базовая информация о турах, возможность связаться с компанией. Продвижение таких сайтов на рынок происходит только в пик сезона и по необходимости активизировать рекламную кампанию. Такие действия не носят систематический характер;

- 10 % – «фирма-клиенту» – сайты, рассчитанные на конечные продажи со страниц сайта, позиционирование в Интернет носит постоянный характер. В белорусском секторе Интернет к таким ресурсам относятся сайты компаний «Альфа-Тур», СМОК, «Экотур-6», «ЭкологияТур», «Белый Дельфин» и пр.

В качестве заключения хотелось бы обратить внимание на один важный момент, препятствующий в значительной степени развитию IT-сферы в туризме – это функциональная безграмотность руководителей большинства туристических предприятий, что выражается в неспешности реакции руководителей и начальников отделов туристических компаний за развитием информационных технологий в туризме. Единственно верным шагом на пути преодоления этой проблемы является повышение квалификации представителей туристических компаний на основе проведения специализированных семинаров, тренингов, консультаций.

## **МЕЖДУНАРОДНОЕ ПРАВО И НАЦИОНАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО ГЕРМАНИИ О ЗАЩИТЕ ИНФОРМАЦИИ О ЛИЧНОЙ ЖИЗНИ ГРАЖДАН**

**О. О. Бельская**

Система защиты данных была создана в Германии около тридцати лет назад. Германские специалисты по защите данных не нашли ни в одной другой стране соответствующих законодательных моделей. Они стали первопроходцами в совершенно новой области права. В основе развития

системы защиты данных лежало политико-психологическое стремление преодолеть настороженность граждан по отношению к государственному планированию и его инструментам, что привело к разработке нового индивидуального права конституционного уровня.

Статья 10 Основного закона Германии гласит: «(1) Тайна писем, почтовых отправлений и телекоммуникаций нерушима. (2) Ограничения могут быть наложены в соответствии с законом.»

Самая первая правовая норма в области защиты данных не только в Федеративной республике, но и во всем мире была принята в 1970 году.

Земельное правительство Гессена разработало законопроект о защите данных в области административного управления. Этот закон преследовал две цели: он должен был, во-первых, предотвратить вторжение в частную сферу граждан с помощью новой информационной техники, а во-вторых, не допустить изменения определенного конституцией разделения полномочий в связи с возникавшим «информационным преимуществом» исполнительных органов власти перед парламентскими органами.

Принятый в Гессене закон касался только защиты личных данных гражданина от вмешательства государства.

Обсуждение проекта Федерального закона о защите данных, который касался как органов федерального управления, так и каждого гражданина, началось в 1971 году. Но принять этот закон удалось только шесть лет спустя.

В 1977 году был принят Федеральный закон о защите данных (BDSG), который претерпел изменения в 1990, 1994 и 1997 годах. Основная цель этого закона – «защита личности от нарушения права человека на свободу *Persönlichkeitsrecht* путем злоупотреблений с персональными данными». Федеральный закон о защите данных разрешил обработку данных только в случаях, определенных законом, или с согласия гражданина, что дает ему возможность проконтролировать этот процесс и закрепил право граждан на информационное самоопределение.

Спустя двенадцать лет после обоснования учеными права на «информационное самоопределение» оно было также признано высшей судебной инстанцией страны после вердикта Федерального конституционного суда 1983 года.

Общественные и частные учреждения должны по требованию гражданина информировать его, какими данными о нем, подпадающими под защиту, они располагают. Это касается также сведений об источнике информации и ее получателе. Эта информация должна предоставляться письменно, в ясной форме и бесплатно.

Наряду с возможностями, которые закон предоставляет каждому отдельному гражданину для проверки своих данных, он предусматривает также наличие контрольных инстанций. Наряду с внутренним контролем закон предусматривает также внешний контроль. Осуществление внешнего контроля в сфере общественного управления входит в обязанности Федерального уполномоченного по защите данных. Его избирает Германский Бундестаг. Федеральный уполномоченный по защите данных избирается на пять лет и может быть переизбран еще на один срок. Федеральный уполномоченный никому не подчиняется и руководствуется только законом.

Одна из основных задач Федерального уполномоченного заключается в том, чтобы проверять личные жалобы граждан об использовании их личных данных федеральными государственными учреждениями и информировать подавшее жалобу лицо о результатах проверки.

Каждое предприятие, на котором заняты, как минимум, пять работников на автоматизированной или 20 человек на ручной обработке личных данных, должно иметь собственного Уполномоченного по защите данных. Он подчиняется непосредственно руководству и больше никому в иерархической структуре предприятия.

Федеральная Комиссия по защите данных (Bundesbeauftragte für den Datenschutz) контролирует соблюдение Закона о защите данных. Основная роль Комиссии – получение и рассмотрение жалоб, подготовка рекомендаций для парламента и других государственных органов.

Другой важный федеральный закон Германии – так называемый G-10, который накладывает ограничения на засекречивание некоторых видов коммуникаций. К этому закону в 2001 году были приняты поправки. Согласно поправкам, провайдеры Интернета должны предоставлять правоохранительным органам возможность вести мониторинг коммуникаций и голосовых каналов связи.

В октябре 2001 года правительство Германии приняло закон (вступит в силу в 2005 году), по которому провайдеры (в том числе и беспроводной связи) должны будут установить оборудование для доступа спецслужб к большей части коммуникаций Германии. Интернет-провайдеры, однако, не подпадают под действие этого закона.

Прослушивание также регулируется законом G-10, по которому оно может быть предпринято при расследовании уголовных преступлений по решению суда.

1 августа 1996 года в Германии вступил в силу новый Закон о средствах телекоммуникации. Он стал необходим, потому что с 01.01.1998 государство утратило свою монополию в данной области в пользу много-

численных частных компаний, в пользу одной из которых телефонные абоненты теперь могут делать свой выбор. Понятие тайны телефонных разговоров было конкретизировано. Например, данные о том, с какого телефонного номера производится звонок, могут передаваться фирмам, занимающимся «телешопингом», только с согласия абонента. Противозаконное прослушивание телефонных разговоров, например, в системе сотовой связи, новым законом запрещено и может караться лишением свободы сроком до двух лет.

Закон об информационных и коммуникационных службах (Закон о мультимедиа) 1997 года устанавливает гарантии защиты данных, используемых в компьютерных сетях. Несмотря на эти гарантии, результаты опроса, проведенного в сентябре 2001 года, показали, что двое из пяти владельцев компьютеров в Германии в возрасте свыше 14 лет не пользуются Интернетом из соображений безопасности.

В июне 2001 года Министерство экономики и технологии Германии предложило компьютерную программу для обеспечения анонимности пользователей при осуществлении платежей через Интернет. В 2002 году эта программа стала доступна широкому кругу потребителей. Эта работа является частью проекта под названием «Защита данных в телекоммуникационных службах» (Data Protection in Teleservices, DASIT), цель которого – развивать программное обеспечение для претворения в жизнь требований законов о защите приватности.

#### **МЕЖДУНАРОДНОЕ ПРАВО И ЕВРОПЕЙСКАЯ ДИРЕКТИВА ПО ЗАЩИТЕ ДАННЫХ 1995 ГОДА.**

Первые в мире нормативы по защите данных, имеющие юридическую силу для многих государств, были приняты странами-партнерами по Европейскому союзу (ЕС). Это позволило обеспечить единообразный подход к использованию данных в рамках внутреннего европейского рынка, поэтому каждый гражданин ЕС, каждое учреждение и каждое предприятие могут быть уверены, что во всем Евросоюзе действуют одинаковые нормы защиты данных.

Соответствующая Директива 95/46/EG, принятая в октябре 1995 года, требовала включить эти нормы в национальное законодательство в течение трех лет. Некоторые страны, включая Германию, не смогли соблюсти этот срок. Тем не менее, нормы, регулирующие взаимоотношения между гражданином и государством, уже сейчас обладают прямым действием, без участия национальных законодателей, поэтому каждый гра-

жданин может непосредственно ссылаться на права, которые ясно определены и гарантированы в Директиве ЕС.

Это прежде всего касается принципиального запрета на обработку так называемой «sensitive data» «чувствительной» информации. При этом имеются в виду все сведения, касающиеся расового и этнического происхождения, политических и мировоззренческих взглядов, здоровья и сексуальной жизни. Так, например, сведения о состоянии здоровья работника не могут без его согласия быть переданы работодателю.

После сентябрьской трагедии 2001 года в США Германия предприняла ряд шагов против терроризма. В январе 2002 года вступил в силу Закон о борьбе с терроризмом, который существенно изменил действующее законодательство. Среди наиболее важных изменений – создание законодательной базы для использования биометрических данных в паспортах и карточках идентификации, упрощения механизма обмена информацией между государственными органами, предоставление секретным службам права на истребование у провайдеров, авиалиний и туристических агентств информации об их пользователях, создание базы данных образцов голоса. В феврале 2002 года Министр внутренних дел объявил, что антитеррористические меры будут включать введение биометрических ID-карточек для всех граждан страны (с использованием шифрования), а также более широкое распространение систем контроля, основанных на дактилоскопии и анализе внешности. Уже известно несколько случаев, когда граждане протестовали против этих нововведений. Германия является членом Совета Европы, подписала и ратифицировала Конвенцию о защите личности в связи с автоматической обработкой персональных данных (ETS No. 108), а позднее и дополнительный протокол к Конвенции. Германия подписала и ратифицировала Европейскую Конвенцию о защите прав человека и основных свобод, в ноябре 2002 года Германия подписала Конвенцию о киберпреступности.

## **KRYPTOGRAFIERECHTLICHE ASPEKTE GLOBALER UNTERNEHMENSKOMMUNIKATION**

**О. О. Бельская**

**Kryptographie** (aus dem griechischen *kryptós*, «versteckt», und *gráphein*, «schreiben») ist die Wissenschaft der Verschlüsselung und Verschleierung von Informationen («Geheimschriften»). Sie ist ein Teilgebiet der [Kryptologie](#).

Bei der Kryptografie geht es um die Idee, wichtige Informationen vor anderen Personen zu verbergen. Dabei bedient man sich der Chiffrierung, also