Глава 15

Информационная безопасность

15.1. Национальные интересы РФ в информационной сфере. Нормативно-правовое обеспечение информационной безопасности РФ

Трудно найти такую сферу знаний и жизни, где бы не использовалась информация. Все более востребованными становятся информационные технологии. Для полноценного развития общества необходима доступность информационных ресурсов, но в то же время информация нуждается в защите.

Анализируя сущность информационной безопасности, нельзя не упомянуть об ***информации*** как объекте правоотношений. Анализ нормативно-правовых актов указывает на определенную закономерность. В федеральных законах, указах, распоряжениях, постановлениях, иных правовых актах термин «информация» приобретает все больший вес.

Фундаментальное право на информацию закреплено в п. 4 ст. 29 гл. 2 Конституции РФ: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом».

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ дает легальное определение понятия «информация»: это сведения (сообщения, данные) независимо от формы их представления. В некоторых отраслях права используются новые термины, производные от понятия информации, например, категории служебной и коммерческой тайны. Уголовный кодекс РФ 1996 г. вводит в российское законодательство понятие «компьютерная информация». Термин «информация» используется в Законах «Об акционерных обществах», «О безопасности», «О внешней разведке», «О Конституционном Суде Российской Федерации».

Статья 128 Гражданского кодекса РФ определяет информацию как объект гражданских правоотношений. Рассматривая информацию с этих позиций, необходимо обращать внимание на особенности юридической защиты информации как объекта права собственности. Исторически традиционным объектом права собственности является материальный предмет. Информация, не являясь материальным объектом окружающего мира, неразрывно связана с физическим субстратом: это мозг человека или отчужденные от него материальные носители (книга, дискета и др.). Рассматривая информацию как отражение действительности человеком, можно

говорить об информации как о некой неовеществленной материи, проявляющейся только при наличии носителя.

В Концепции национальной безопасности РФ под национальными интересами России понимается совокупность сбалансированных интересов личности, общества и государства в экономической, внутриполитической, социальной, международной, информационной, военной, пограничной, экологической и других сферах. Они носят долгосрочный характер и определяют основные цели, стратегические и текущие задачи внутренней и внешней политики государства.

В современном мире суверенности государств и наций угрожают новые опасности, связанные с информационной сферой. Информация, которая играет ведущую роль в развитии современного государства и общества, может подвергаться преднамеренному или непреднамеренному искажению, порче, уничтожению — и все это будет отрицательно сказываться на благосостоянии нации и ее отдельных представителей. Поэтому сегодня информационная сфера включена в число объектов, нуждающихся в защите в целях сохранения целостности общества и государства. Таким образом, информационная безопасность Российской Федерации является частью системы национальной безопасности.

В Указе Президента РФ «О концепции национальной безопасности Российской Федерации» от 10.01.2000 г. № 24 интересы России в информационной сфере впервые были упомянуты как составная часть национальной безопасности.

Концепция национальной безопасности РФ определяет, что национальные интересы России в информационной сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа. Концепция предусматривает также защиту культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни. Но наиболее полно понятие информационной безопасности отражено в **Доктрине информационной безопасности РФ** от 09.09.2000 г. № Пр-1895, развивающей основные положения Концепции национальной безопасности РФ применительно к информационной сфере. Она состоит из четырех разделов и включает в себя 11 глав.

Содержательно Доктрина раскрывает понятие информационной безопасности Российской Федерации, ее национальные интересы в информационной сфере, виды и источники угроз информационной безопасности Российской Федерации, состояние информационной безопасности РФ и основные задачи по ее обеспечению, общие методы обеспечения информационной безопасности Российской Федерации; особенности их применения в различных сфе-

рах общественной жизни, международное сотрудничество РФ в области информационной безопасности, принципы организации системы ее обеспечения в РФ.

Под *информационной безопасностью* Российской Федерации здесь понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере связаны с реализацией конституционных прав человека на доступ к информации и на ее использование для осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития. Отдельно можно выделить право на защиту личной или иной информации, обеспечивающей физическую и психологическую безопасность человека.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой области, а также упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия. В качестве особой задачи Доктрина выделяет духовное обновление России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние. К внешним источникам относятся:

– деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов РФ в информационной сфере;

– стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

– обострение международной конкуренции за обладание информационными технологиями и ресурсами;

– деятельность международных террористических организаций;

– увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

– деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

– разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира;

– нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

– критическое состояние отечественных отраслей промышленности;

– неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

– недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;

– недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

– неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

– недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

– недостаточная экономическая мощь государства;

– снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

– недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

– отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

15.2. Общие направления и методы обеспечения информационной безопасности

Можно говорить о двух главных направлениях обеспечения информационной безопасности. Первое связано с нейтрализацией отрицательного влияния на интеллектуальный, духовный и психологический потенциал общества; данное направление принято обозначать как *информационно-психологическое*. Главными объектами защиты здесь являются психика представителей элиты и населения страны в целом, а также система формирования общественного сознания и общественного мнения и процессы принятия решений. Можно выделить три вида объектов, которым может быть нанесен вред с помощью информационного воздействия.

• Индивидуальное сознание человека. Для нормального функционирования общества и государства необходимо, чтобы составляющие его индивиды обладали способностью адекватно воспринимать окружающую действительность, свое место в мире, формировать на основе своего жизненного опыта определенные убеждения, принимать решения и совершать действия в соответствии с ними. Поэтому основной угрозой индивидуальному сознанию будет нарушение этой способности с помощью различных способов воздействия на сознание и подсознание человека.

• Групповое сознание. Группы (социальные, профессиональные, этнические, религиозные) являются одним из путей объединения индивидов для достижения определенных целей, которые разделяют все члены группы. Объединение в группы может происходить как стихийно, так и целенаправленно. Создание и функционирование социальных общностей (групп людей, объединенных по определенному признаку) — естественный способ существования человека, поскольку достижение сложных социальных целей для индивидов зачастую возможно только в группе. Угрозы групповому сознанию могут проявляться в виде противоправных информационных воздействий со стороны других групп, общественных или государственных организаций с целью разрушения общности интересов группы, создания трудностей на пути реализации этих интересов, дискредитации членов группы, оказания психологического давления на них.

• Массовое сознание. Под массовым сознанием при рассмотрении проблем информационной безопасности мы понимаем совокупность общих интересов социальных общностей, проживающих на территории страны, признаваемых ими культурных, духовных и нравственных ценностей, сложившихся нравов, устанавливающих общественно допустимые правила поведения и образ жизни; все эти составляющие массового сознания одновременно присутствуют в индивидуальном и групповом сознании представителей дан-

ного общества. Таким образом, все информационные воздействия, которые разрушают культурные, духовные и нравственные ценности, разделяемые большинством граждан страны, а также различные искажения информации о происходящих в ней событиях и окружающем мире, которые могут нарушить способность граждан страны социализироваться и нормально функционировать в данном социуме и государстве, являются информационной угрозой массовому сознанию.

В качестве основных средств информационно-психологического воздействия на человека выделяются следующие:

– средства массовой коммуникации (в том числе информационные системы, например Интернет и т. п.);

– литература (художественная, научно-техническая, общественно-политическая, специальная и т. п.);

– искусство (например, различные направления так называемой массовой культуры и т. п.);

– образование (государственные и негосударственные системы дошкольного и среднего общего образования, начального, среднего и высшего профессионального образования);

– воспитание (разнообразные формы воспитания в семье, образовательных учреждениях, общественных организациях — формальных и неформальных, система социальной работы и т. п.);

– личное общение.

Второе направление обеспечения информационной безопасности связано с функционированием и развитием информационной инфраструктуры государства, радиоэлектронной промышленности и сферы высоких технологий. Это направление может быть названо *информационно-техническим*, и главными объектами защиты здесь становятся системы связи и телекоммуникаций, радиоэлектронные средства и т. д. Таким образом, под информационно-технической безопасностью можно понимать состояние защищенности информационно-технических систем страны.

Общие методы обеспечения информационной безопасности, как правило, разделяются на правовые, организационные и технические.

К правовым методам следует отнести разработку норм, устанавливающих ответственность за преступления в информационной сфере, совершенствование уголовного и гражданского законодательства, а также судопроизводства. Правовые методы включают также ратификацию международных договоров об ограничении доступа к информации, способной повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашение.

Организационными методами считают: меры по охране объектов информационной безопасности; подбор надежного персонала; исключение ситуаций, когда особо важные работы ведет только один человек; создание планов восстановления работоспособности подразделений, занимающихся обработкой и хранением информации, на случай выхода их из строя; организацию обслуживания информационных систем; разработку универсальных средств защиты информационных систем и т. п.

К техническим методам можно отнести: защиту от несанкционированного доступа к системе с помощью паролей; резервирование особо важных компьютерных подсистем; обеспечение возможности перераспределения ресурсов в случаях, когда нарушается работоспособность отдельных звеньев вычислительных сетей; установку оборудования для обнаружения и ликвидации пожара или протечки воды; конструктивные меры защиты от хищений, саботажа, диверсий, взрывов; предусмотрение резервных систем электропитания; оснащение помещений замками; установку сигнализаций и др.

15.3. Методы и средства защиты электронной информации

Возможные угрозы и противоправные действия в этой сфере можно предупредить различными методами и средствами, начиная от создания здорового климата в коллективе и заканчивая прочной системой защиты, обеспечиваемой физическими, аппаратными и программными средствами.

Защитные действия можно классифицировать:

– по содержанию и характеру информации (персональная, финансовая, техническая информация);

– по характеру угроз (разглашение, утечка, несанкционированный доступ);

– по направлениям (правовое, организационно-техническое, инженерное);

– по способам действий (предупреждение, обнаружение, пресечение, восстановление);

– по охвату (территория, здание, помещение, аппаратура, элементы аппаратуры);

– по масштабу (объектовая, групповая, индивидуальная).

Средства защиты электронных данных:

– многоуровневый контроль доступа (идентификация пользователя, допуск в систему, к данным, к задачам);

– уровни защиты данных (информационная база данных, информационный массив, набор, запись, поле);

– тип замка (ключевой — применение единого ключа, физического или электронного; процедурный — прохождение авторизации (подтверждение статуса пользователя) и идентификации (определение самого пользователя));

– вид пароля (статический — ключ; разовый — используемый при защите передаваемой конкретной информации, файлов, папок с файлами и т.д.; изменяемый — используется пользователем, администратором для защиты компьютеров);

– динамическая проверка защищенности (в момент открытия базы, в момент подтверждения разрешения на обмен данными).