Елин В.М.

Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом

Монография

Под редакцией Баранова А.П.

Работа выполнена по Гранту РГНФ «Сравнительно-правовое исследование методов обеспечения информационной безопасности в РФ и странах-членах ЕС» № 16-03-00679

УДК 341.231
ББК 67. 404. 2
Е51
ISBN 978-5-9909450-7-4
Рецензенты:

Стрельцов Анатолий Александрович, Заместитель Директора Института проблем информационной безопасности МГУ имени М.В.Ломоносова, Заслуженный деятель науки Российской Федерации, доктор технических наук, доктор юридических наук, профессор

Бабаш Александр Владимирович, доктор физико-математических наук, профессор

Под редакцией академика Академии криптографии, доктора физико-математических наук, профессора Баранова Александра Павловича

Автор:

Елин Владимир Михайлович, доцент кафедры информационной безопасности НИУ ВШЭ, кандидат наук

Елин В.М. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом: Монография

Монография посвящена анализу стратегических документов и нормативно-правовых актов Российской Федерации, США, Евросоюза и НАТО, разработанных и принятых в целях правового регулирования информационной безопасности государств и их объединений. В работе раскрываются особенности организационно-правового регулирования системы информационной безопасности как составной части государственной безопасности. При этом освещается ряд аспектов обеспечения информационной безопасности с помощью гражданско-правовых и уголовно-правовых средств, а также ряд особенностей обеспечения безопасности некоторых категорий информации. Текст монографии включает исследовательские, научные работы автора и рассчитан на широкий круг читателей.

Работа выполнена по гранту РГНФ «Сравнительно-правовое исследование методов обеспечения информационной безопасности в РФ и странах-членах ЕС» № 16-03-00679

Материал подготовлен с использованием информационно-поисковой системы «Консультант Плюс» (www.consultant.ru)

Оглавление

Введение....4

Глава 1. Формирование концепций правового регулирования информационной безопасности за рубежом и в России....10

1.1. Системность подхода к построению Стратегии кибербезопасности в США....10

1.2. Национальные стратегии кибербезопасности в странах ЕС и НАТО....25

1.3. Стратегия формирования правовых методов информационной безопасности Российской Федерации....43

Глава 2. Правовые методы обеспечения информационной безопасности....58

2.1. Характеристика информации, как объекта обеспечения безопасности в Российской Федерации....58

2.2. Гражданско-правовые механизмы обеспечения информационной безопасности....92

2.3. Значение ноу-хау и режима коммерческой тайны в практической деятельности обеспечения информационной безопасности....109

2.4. Система уголовно-правового обеспечения информационной безопасности....123

Глава 3. Правовое регулирование некоторых сфер информатизации в России и за рубежом....139

3.1. Защита приватности и персональных данных в законодательстве России и США....139

3.2. Электронный документ в России и США....161

Введение

Начало 2-го тысячелетия характеризуется широким применением информационно-коммуникационных технологий (ИКТ) и внедрением инновационных средств производства. Положенная в основу нового общественного уклада концепция экономики знаний базируется на постулате о том, что в основе дальнейшего общественного развития лежит осознанная необходимость повышения технологического уровня производства и распространения современных информационных и телекоммуникационных технологий[1]. Указанная тенденция отражена целым рядом программных документов международного сообщества, носящих декларативный характер: Хартией глобального информационного общества (2000 г.)[2] Декларацией о свободе обмена информацией в Интернете (Совет Европы 28 мая 2003 г.)[3]; Европейской декларацией о правах человека и верховенстве права в информационном обществе (2005 г.)[4] Соглашением между странами СНГ о сотрудничестве в области информации от 9 октября 1992 г.[5]; Декларацией принципов построения информационного общества 2003 г и др.

Развитие информационных технологий порождает обоснованное мнение[6] о состоянии перехода к шестому экономическому укладу, постиндустриальному обществу новой формации, где все большое значение приобретают информационные и телекоммуникационные технологии, проникающие во все сферы общественной и частной жизни. Наличие информации становится показателем успешности политической,

---

[1] Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 07.02.2008 № Пр-212) // РГ, № 34, 16.02.2008

[2] Хартия глобального информационного общества 2000 г. //Дипломатический вестник. 2000. № 8. С. 51 - 56.

[3] Декларация Совета Европы от 28 мая 2003 г. О свободе обмена информацией в Интернете //Документ в России официально опубликован не был (см. в справочной правовой системе "Консультант Плюс"). официальный текст на английском языке: https://wcd.coe.int/ViewDoc.jsp?id=37031&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

[4] Европейская декларация о правах человека и верховенстве права в информационном обществе // http://www.ifap.ru/ofdocs/eu/dhrrlis.pdf.

[5] Соглашением между странами СНГ о сотрудничестве в области информации от 9 октября 1992 г // Бюллетень международных договоров. 1993. № 10.

[6] Перес К. Технологические революции и финансовый капитал: Динамика пузырей и периодов процветания. Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages— М.: Дело, 2011.— 232 с.; Садовничий В.А., Акаев А.А., Коротаев А.В., Малков С.Ю., Моделирование и прогнозирование мировой динамики. — М.: ИСПИ РАН, 2012.— 359 с.; Techno-Economic Paradigms: Essays in the Hounor of Carlota Peres / Ed. By Wo. Drechsles etc. — London: Anthem Press, The other Canon Foundation, 2011. — 442 с.

общественной, либо хозяйственной деятельности. Появляются и активно используются узконаправленные (слабые) искусственные интеллекты, которые (в отличие от общих (сильных) искусственных интеллектов и искусственных сверхинтеллектов) ориентированы на решение задач в одной области (поисковые системы, управление автомобилем т.д.). При этом уже сейчас слабым искусственным интеллектам передается возможность принятия решений, влекущих за собой возникновение, изменение или прекращение правоотношений.

Особенностью современных информационных технологий выступает возможность их использования участниками вне зависимости от уровня технической грамотности и подготовленности субъектов. Максимально «дружелюбные» интерфейсы, комфортные языки программирования, доступность программ и компьютерного оборудования порождают активную деятельность широкого круга лиц в информационной сфере. В то время как информационные технологии усложняются и совершенствуются, активные пользователи технологий катастрофически утрачивает как знания, так и рычаги воздействия на техногенную среду. Возникает общество пользователей, получающих блага от используемых технологий.

При этом четко прослеживается проблема использования информационных ресурсов, основанная на внутреннем противоречии информационного общества, для которого, с одной стороны, право на информацию является обязательным компонентом обеспечения общественной жизни, с другой стороны, информация выступает в качестве ценного продукта, требующего значительных затрат в производстве, реализация которого предполагает получение выгоды в той или иной форме.

Возможность практического применения информационных технологий в готовом виде без понимания сущности процессов, порождает, в том числе, конфликт определения статуса участников и возможностей установления порядка протекания ИТ-процессов в обществе[7].

Вопрос о форме и методах правового регулирования информационных технологий порождает конфликт между «юристами» и «технарями», схожий со спорами между физиками и лириками в 60-е годы прошлого века. В основе конфликта лежит схожесть позиции об избыточности правового

[7] Жарова А.К. Право и информационные конфликты в информационно-телекоммуникационной сфере. – М.: Янус К. 2016. — 435 с.

регулирования в процессе применения информационных технологий. При этом позиция специалистов в области информационных технологий («технарей»), упускает из вида то обстоятельство, что указанные технологии получены российским обществом с готовой программной, элементной, технологической и правовой базой, что делает невозможным применение имеющегося у наших граждан житейского и правового опыта в процессе их применения и использования.

«Юристы» основывают свою позицию на постулате о том, что правовое регулирование в области информационных технологий прекрасно вписывается в существующую систему и не требует разработки новых подходов. При этом ряд российских юристов[8] ссылается на американского судью, который соотносит cyberlaw (киберправо, интернет-право) с «лошадиным правом»[9], оставляя за рамками внимания как контрааргументацию известнейшего теоретика и практика Л. Лессига[10], так и совокупность американских правовых норм, de-facto, создавших отрасль Information Technologies Law.

Результатом указанной рассогласованности является отсутствие единого теоретического взгляда на концепцию правового обеспечения информационной безопасности в нашей стране, бессистемность подхода к нормативно-правовой деятельности, отсутствие практики правового обеспечения информационной безопасности.

В результате наблюдается отрыв правовых норм от реальности применения технологических процессов в области информационных технологий. Например, применяемый в нашей стране международный стандарт по информационной безопасности, разработанный совместно Международной организацией по стандартизации и Международной электротехнической комиссией и ISO/IEC 27001[11] вступает в конфликт с нормами российского права уже на уровне понятийного аппарата.

---

8 Талапина Е.В. О возможностях правового регулирования Интернета. Труды института государства и права РАН. № 3 (55). М., 2016; Богдановская И.Ю. Информационно-коммуникационные технологии и развитие правового понятийного аппарата (сравнительно-правовые аспекты). Понятийный аппарат информационного права. Сборник научных работ. М, 2015, с. 49-56.

9 Easterbrook, Frank H. (1996).Cyberspace and the Law of the Horse (PDF).*University of Chicago Legal Forum*. Retrieved October 5,2009. // https://www.law.upenn.edu/fac/pwagner/law619/f2001/week15/easterbrook.pdf

10 Lessig. Lawrence (1999). The Law of the Horse: What Cyberlaw Might Teach(PDF). 113 Harv. L. Rev. 501. Retrieved October 5, 2009. // https://cyber.law.harvard.edu/works/lessig/finalhls.pdf

11 ISO/IEC 27001 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.» // СПС Консультант плюс

Особую опасность представляет возможность злоупотребления правомочиями. Так, наличие на территории Российской Федерации более 400 удостоверяющих центров электронной подписи не только способствуют развитию услуг, но и повышает риск недобросовестной защиты данной категории информации. В США таких центров всего пять, в т.ч. из-за угрозы инсайдерской утечки информации. Проблема добросовестности участников приобретет особую актуальность, поскольку достаточно небольшой погрешности в работе программ, чтобы открылись «бреши для злонамеренного использования электронной подписи»[12].

Прослеживается проблематика информационной безопасности в процессе осуществления хозяйственной деятельности, сопряженной с проблемами сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации, в которых наиболее опасны противоправное копирование информации и ее искажение.

И наконец, возрастает угроза информационной безопасности в личной и семейной жизни граждан, при защите их персональных данных, поскольку имеет место формальность применения правовых норм как в сфере информационных технологий, так и в сфере защиты персональных данных.

При возрастании значимости информации актуализируется вопрос о возможности обеспечения ее безопасности на всех уровнях, в т.ч. об информационной безопасности государства. При этом, по мнению А.А.Стрельцова, информационная безопасность дуалистически является результатом деятельности по ее обеспечению и состоянием защищенности человека, общества и государства в информационной сфере. Отсюда возникает необходимость деятельности по противодействию угрозам безопасности человека, общества и государства в информационной сфере, осуществляемой с использованием выделяемых для этого сил и средств[13].

Поскольку Стратегия развития информационного общества в Российской Федерации ставит задачу «обеспечения национальной

12 Баранов А.П. Налоговая подпись и пространство доверия // Налоговая политика и практика. 2012. № 5. С. 66-69.

[13] Организационное и правовое обеспечение информационной безопасности. Учебник и практикум для бакалавриата и магистратуры . Под.ред. Т.А.Поляковой, А.А.Стрельцова, М., 2016. С. 15

безопасности в информационной сфере»[14], а Доктрина информационной безопасности Российской Федерации[15] относит правовые средства к числу мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления, следует уделить внимание ряду вопросов:

- о специфике правового метода обеспечения информационной безопасности;
- о правовом инструментарии обеспечения информационной безопасности;
- о возможности использования зарубежного опыта в разработке и принятии документов стратегического планирования Российской Федерации в области информационной безопасности;
- о возможности имплементации международных правовых норм в российскую правовую систему.

Для получения ответов на поставленные вопросы в настоящей работе :

- проанализировано действующее законодательство Российской Федерации и зарубежных стран в области обеспечения информационной безопасности;
-исследовано становление и развитие правового обеспечения информационной безопасности в Российской Федерации и за рубежом;
- осуществлен анализ правовой системы обеспечения информационной безопасности в Российской Федерации;
- исследован правовой режим обмена информацией в сети интернет и электронный документооборот с точки зрения обеспечения информационной безопасности;
- определено место и роль защищаемой информации ограниченного доступа в системе информационной безопасности;
- предложен унифицированный подход к определению признаков правового режима информации ограниченного доступа;

[14] "Стратегия развития информационного общества в Российской Федерации" (утв. Президентом РФ 07.02.2008 № Пр-212) // РГ, № 34, 16.02.2008

[15] Доктрина информационной безопасности Российской Федерации // Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ, 12.12.2016, № 50, ст. 7074

- рассмотрены особенности документированной информации в электронной форме как объекта правового регулирования информационного, гражданского и уголовного права, подлежащего правовой защите.

Текст монографии содержит результаты ряда научных исследований.

Работа выполнена по гранту РГНФ «Сравнительно-правовое исследование методов обеспечения информационной безопасности в РФ и странах-членах ЕС» № 16-03-00679.

Глава 1. Формирование концепций правового регулирования информационной безопасности за рубежом и в России

1.1. Системность подхода к построению Стратегии кибербезопасности в США

В основе подхода Соединённых Штатов Америки к проблемам международного киберпространства лежит убежденность в том, что технологии обладают огромным потенциалом для страны и мира, поскольку основываются на достигнутых успехах и признании задач национальной и экономической безопасности. Киберпространственная среда поощряет инновации и поддерживает предпринимателей; соединяет индивидуумов и усиливает сообщества; создаёт лучшие правительства и способствует отчётности; стоит на страже основных свобод и в наибольшей мере обеспечивает право частной жизни; способствует пониманию, проясняет нормы поведения и усиливает национальную и международную безопасность.

Подписанная Президентом США в 2011 году **International Strategy for cyberspace (Prosperity, Security and Openness in a Networked World** [16](Международная стратегия по действиям в киберпространстве (Процветание, безопасность и открытость в сетевом мире) раскрывает видение будущего киберпространства и план сотрудничества между странами и народами с целью его реализации. В International Strategy for cyberspace определено доминирующее положение США в современном киберпространстве, фактически монополизируя право определять правильность поведения в условиях информационного общества.

International Strategy for cyberspace определяет четыре определяющих характеристики:

- открытость для инноваций;
- взаимодействие по всему миру;

[16] International Strategy for cyberspace (Prosperity, Security and Openness in a Networked World, 22-05-2011 // https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

- безопасность, заслуживающая доверия людей;
- надёжность, способная поддержать работу.

В целях реализации указанных идей, США декларирует в International Strategy for cyberspace возможность строить и поддерживать среду, в которой нормы ответственного поведения участников служат ориентиром для государств, укрепляют партнерство и поддерживают верховенство закона. Эти нормы включают в себя:

- поддержку основных свобод;
- уважение к собственности;
- ценность личной жизни;
- защиту от преступлений;
- право на самооборону;
- глобальную совместимость;
- сетевую стабильность;
- надёжность доступа;
- участие множества сторон в управлении;
- должное внимание к кибербезопасности.

International Strategy for cyberspace определяет, что Соединённые Штаты Америки планируют противостоять тем, кто попытается разрушать сети и системы, а также будут демотивировать и сдерживать злоумышленников, сохраняя за собой право защищать эти важные национальные активы необходимыми и адекватными методами.

При более сложных, наносящих определённый ущерб атаках, США планирует реагировать в соответствии с планами по локализации и смягчению наносимого ущерба, ограничивая его эффект на сети и возможный каскадный эффект в дальнейшем. В случае необходимости Соединённые Штаты Америки будут реагировать на враждебные действия в киберпространстве так же, как реагировали бы на любую другую угрозу в стране, оставляя за собой право использовать любые средства — дипломатические, информационные, военные и экономические. При этом по возможности будут избегать военного вмешательства прежде, чем все другие варианты будут исчерпаны и будут укреплять легитимность, опираясь по возможности на широкую международную поддержку.

Стратегия США содержит приглашение другим государствам и народам присоединиться к реализации идеи процветания, безопасности и открытости в цифровом мире США. Программа позволит агентствам и департаментам правительства Соединённых Штатов Америки лучше определять и координировать свою роль в международной киберпространственной политике.

Деятельность правительства Соединённых Штатов структурируется по семи областям, что создаст структуру стратегических направлений в следующих областях жизнедеятельности.

В области экономики:

- поддержка свободного рыночного окружения, поощряющего технологические инновации через доступные, глобально связанные сети;
- защита интеллектуальной собственности, в том числе коммерческой тайны;
- обеспечение верховенство совместимых и безопасных технических стандартов, устанавливаемых техническими экспертами.

В области защиты сетей:

- повышение безопасности, надёжности и устойчивости;
- стимулирование сотрудничества в киберпространстве в двухстороннем и многостороннем порядке (в частности в области норм поведения государств и кибербезопасности) с участием заинтересованных организаций и многонационального партнёрства;
- борьба за уменьшение числа вторжений в сети США и срывов их работы;
- обеспечение оперативного реагирования на происшествия, устойчивости и возможности восстановления информационной инфраструктуры;
- повышение надёжность высокотехнологической цепи поставок.

В области правоприменения:

- расширение сотрудничества и верховенство закона:
- принятие участия в развитии международной политики по киберпреступности;
- согласование законов о киберпреступности на международном уровне через расширение поправок к Будапештской конвенции;
- определение в качестве целей законов о киберпреступности борьбы с нелегальной деятельностью, а не ограничение доступа в интернет;

- лишение террористов и прочих преступников возможности использовать интернет для планирования и финансирования операций и атак.

В области развития вооруженных сил:

- подготовка к проблемам безопасности XXI века;
- учет растущих потребностей вооруженных сил в надёжных и безопасных сетях, и возможность приспосабливаться к этим потребностям;
- создание и усовершенствование существующих военных союзов для противостояния возможным угрозам в киберпространстве;
- расширение сотрудничества с союзниками и партнёрами в киберпространстве с целью повышения общей безопасности.

В области управления интернетом:

- упор на открытость и инновации в интернете;
- сохранение безопасности и стабильности глобальной сети, в том числе и систему доменных имён;
- учреждение конференции между участниками по вопросам управления интернетом и содействие им.

В области международного развития:

- обеспечение стран, желающих создать технический потенциал и потенциал кибербезопасности, необходимыми знаниями, обучением и прочими ресурсами;
- постоянное предоставление лучших наработок в области международной кибербезопасности;
- повышение способности государств к борьбе с киберпреступностью, в том числе путём подготовки правоохранительных органов, судебных специалистов, юристов и законодателей;
- наращивание технического потенциала путем обеспечения постоянных и продолжительных контактов с экспертами и их коллегами из правительства Соединённых Штатов Америки.

В области свободы интернета:

- поддержка основных свобод и частной жизни;
- поддержка деятелей гражданского общества в создании надёжных, защищённых и безопасных платформ для объединения и свободы самовыражения;

- работа над мерами по защите интернет-активности от незаконных цифровых вторжений;
- поощрение международного сотрудничества с целью эффективной защиты коммерчески значимых данных;
- обеспечение сквозной совместимости для всеобщего взаимодействия в интернете.

Таким образом, США определяют для себя роль арбитра и контроллера процессов свободных информационных потоков и обеспечения свободы интернета, связанных со свободным обращением информации в международных сетях и запрете иностранных государств на их ограничение. International Strategy for cyberspace определяет обязательное базирование международного сотрудничества в сфере борьбы с киберпреступлениями на нормах Европейской конвенции о киберпреступности (ETS № 185)[17] также можно отнести к положениям, подрывающим суверенитет иностранных государств. Норма ст. 32 (b) указанной Конвенции закрепляет право получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным. Указанная норма, в свое время послужила основанием отказа от участия РФ в Европейской Конвенции о киберпреступности, в связи с ее угрозой суверенитету страны[18].

Особый интерес в International Strategy for cyberspace представляет норма обеспечения открытости и безопасности киберпространства не только информационными, экономическими и дипломатическими средствами, но также с использованием вооруженных сил США.

В том же контексте рассматривается и проблема «управления Интернетом» - США категорически отвергают идею передачи всех необходимых полномочий наднациональному органу в структуре ООН, отстаивая ведущую роль **Internet Corporation for Assigned Names and Numbers** (ICANN). При этом следует иметь в виду, что ICANN представляет собой международную некоммерческую организацию, созданную при участии правительства США

[17] Convention On Cybercrime. Конвенция о преступности в сфере компьютерной информации (ETS № 185).Заключена в г. Будапеште 23.11.2001. // СПС Консультант плюс

[18] Распоряжение Президента РФ от 15.11.2005 N 557-рп, которое признано утратившим силу Распоряжением Президента РФ от 22.03.2008 N 144-рп

для регулирования вопросов, связанных с доменными именами, IP-адресами и прочими аспектами функционирования Интернета[19].

Оставляя за США право определять правильность поведения в киберпространстве, International Strategy for cyberspace определяет действенность международных норм относимых к киберпространству и определяет возможность США отвечать на кибератаки любыми средствами, в т.ч. оружием со ссылкой на положения Устава ООН о праве государств на самооборону.

В свете событий последнего времени, связанных с использованием сети для насильственного свержения законных правительств, особый интерес представляют нормы Стратегии о работе гражданских активистов. Прямо говорится, что США будут помогать таким «активистам», чтобы повысить безопасность их электронных почтовых ящиков, веб-сайтов, мобильных телефонов и т.д.

Кроме того, Федеральное законодательство США содержит ряд законов, регулирующих правоотношения в области информационной безопасности:

Electronic Communications Privacy Act of 1986 (**Электронный Закон о конфиденциальности электронных коммуникаций 1986 года, ECPA**)[20], котор0ый принят, чтобы определить порядок прослушивания телефонных переговоров и электронных данных, переданных с помощью компьютера. Закон кодифицирован в гл. 18 US Code (§ 2510 и далее). Законом добавлены положения, запрещающие доступ к хранилищам электронных сообщений, и разрешающие отслеживание телефонной связи.

Законом **ECPA** определено, что под электронными средствами связи следует понимать «любую передачу знаков, сигналов, письменного текста, изображений, звуков, данных или информации любого характера, передаваемой в целом или частично по проводам, радио-, электромагнитной, фотоэлектронной или фотооптической системы, за исключением следующих электронных средств:

- приборов проводных или устных сообщений;
- приборов, осуществляющих связь только через устройства тонального поискового вызова (пейджеры);
- сообщения от устройств слежения;

[19] https://www.icann.org/

[20] **Electronic Communications Privacy Act of 1986** // https://www.law.cornell.edu/uscode/text/18/2510

- устройств электронного перевода денежных средств, использующихся финансовым учреждением в системе связи для электронного хранения и перевода средств».

Закон Electronic Communications Privacy Act of 1986 состоит из трех разделов: Раздел 1 Закона ECPA защищает данные в процессе и устанавливает требования производства обысков. Раздел II ECPA, включает другой закон: the **Stored Communications Act of 1986** (Закон о хранении контактов) (далее **SCA) и** направлен на защиту коммуникаций, хранилищ информации, сообщений, хранящихся на компьютерах. Раздел III ECPA запрещает использование записей и регистрацию данных, устройства трассировки, маршрутизации, адресации и передачи сигнальной информации, без постановления суда.

Stored Communications Act of 1986[21] (Закон о хранении контактов **(SCA), кодифицированный в 18 U.S. Code, гл. 121** §§ 2701-2712, предусматривает процедуру добровольного или принудительного раскрытия хранящихся электронных и проводных сообщений и транзакционных записей, принадлежащих провайдерам интернет-услуг (ISP). Закон принят в качестве раздела II **Electronic Communications Privacy Act of 1986** (ECPA).

Stored Communications Act of 1986 определяет возможности Правительства США по принуждению к раскрытию информации и устанавливает две категории услуг:

- Electronic communication service (услуга электронной коммуникации) и
- Remote computing service (дистанционное компьютерное обслуживание).

Для раскрытия информации, относящейся к первой категории, требуется предоставить ордер на обыск с указанием оснований его производства. Для второй категории достаточно повестки в суд или судебного приказа с предварительным уведомлением.

В Stored Communications Act of 1986определено, что информация второй категории соотносится с уровнем защиты, предоставляемой четвертой поправкой Конституции США или меньше указанного уровня защиты, поскольку уведомление может быть отложено на неопределенное время с временным периодом 90 дней.

[21] Stored Communications Act // https://www.law.cornell.edu/uscode/text/18/2701

При этом следует иметь в виду, что четвертая поправка к Конституции США принята в 1792 году и является частью Билля о правах, которая запрещает необоснованные обыски и задержания, требуя наличие достаточных оснований для выдачи ордеров на обыск. До принятия поправки ордера (приказы) давали право обыскивать любые помещения и любых лиц во исполнение цели, описанной в ордере лишь в общих чертах. При этом обыскивающий не был ответственен за ущерб, нанесённый при обыске, а также мог перепоручать обыск другим лицам. Начиная со второй половины двадцатого века суды стали признавать, что четвертая поправка защищает в целом право человека на приватность, а не лишь его физическую неприкосновенность.

Закон Stored Communications Act of 1986 также регламентирует деятельность в случаях, когда электронные данные хранятся за пределами территории, попадающей под юрисдикцию США, в связи с тем, что многие Интернет - провайдеры имеют распределенные по всему миру сервера и центры обработки данных.

Приведем судебную практику, связанную с Законом SCA. Рассматривалось дело Microsoft Corporation vs United States of America, в связи с тем, что 4 декабря 2013 года государственные органы получили повторный ордер на поиск определенной учетной записи электронной почты, контролируемой и поддерживаемой Microsoft Corporation. Представитель компании Microsoft указал, что запрашиваемая информация находится на сервере в Ирландии, в связи с чем Microsoft подала ходатайство об аннулировании ордера, в связи с его экстерриториальным применением. Ходатайство было отклонено судом и на основании SCA, предписание было объяснено как коллизия, которая выполняется как повестка в суд. 14 июля 2016 года Апелляционный суд второго округа США вынес решение в пользу Microsoft, поскольку положения SCA не могут применяться экстерриториально.

Другой прецедент Robbins vs. Lower Merion School District связан с тем, что в 2010 году средние школы Филадельфии шпионили за учащимися путем скрытной и удаленной активации веб - камер, встроенных в ноутбуки учащихся школы, которые те использовали у себя дома, тем самым нарушалось право на частную жизнь учащихся. Школы признали виновными

в осуществлении более 66000 вебшотов[22] и скриншотов[23], в том числе в спальнях учащихся.

Закон - **Federal Information Security Management Act of 2002 (Федеральный закон об управлении информационной безопасностью 2002 года, FISMA,кодифицирован 44 U.S. Code § 3541** и далеее) принят в качестве главы III **the E-Government Act of 2002** (Закона об электронном правительстве 2002 года).

Закон Federal Information Security Management Act определяет важность информационной безопасности в структуре экономической и национальной безопасности Соединенных Штатов. Закон требует от каждого федерального ведомства разработать, документировать и внедрить программу агентства по обеспечению информационной безопасности и безопасности систем, поддерживающей операции и активы агентства. FISMA предъявляет требования к должностным лицам федеральных Агентств, директорам по информационным технологиям, а также генеральным инспекторам (IGS), которые заключаются в обязанности данных субъектов проводить ежегодные обзоры программ информационной безопасности и сообщать о результатах в Бюро управления бюджетом (OMB), являющимся самым крупным офисом в Канцелярии Президента США. Бюро управления бюджетом использует эти данные для осуществления надзорных функций и подготовки ежегодного доклада Конгрессу.

FISMA определяет конкретные обязанности федеральных Агентств, Национального института стандартов и технологий (NIST) и Бюро управления бюджетом в целях укрепления систем информационной безопасности.

Согласно FISMA, термин информационная безопасность означает защиту в целях обеспечения целостности, конфиденциальности и доступности информации и информационных систем от несанкционированного доступа, использования, разглашения, разрушения, модификации или уничтожения..

В соответствии с FISMA, NIST работает в тесном взаимодействии с федеральными Агентствами и отвечает за разработку стандартов, руководств и связанных с ними методов и технологий для обеспечения адекватной информационной безопасности всех операций Агентств и активов, за

[22] Небольшая бесплатная утилита, позволяющая сделать полноразмерные скриншты веб-страниц
[23] Снимки с экрана

исключением системы национальной безопасности., а также публикует стандарты и руководящие принципы, которые обеспечивают основу программ по информационной безопасности в органах государственной власти и управления. NIST разрабатывает и принимает следующие документы: - проект внедрения FISMA;

- программу автоматизации информационной безопасности (ISAP)[24];
- национальную базу уязвимостей [25](NVD), которое состоит из американского правительственного хранилища контента и протокол безопасности контента автоматизации (Security Content Automation Protocol (SCAP))[26].

NVD является хранилищем стандартов США, формируемым на основе данных управления уязвимостями, измерения безопасности и соответствия.

FISMA определяет структуру управления информационной безопасностью, которая должна соблюдаться при работе всех информационных систем, используемых или эксплуатируемых федеральным правительством США, в структурах исполнительной или законодательной ветвях власти.

FISMA устанавливает необходимость инвентаризации информационных систем, предписывает руководителям федеральных Агентств осуществлять разработку и ведение перечня информационных систем (в том числе систем национальной безопасности) в ведении или под контролем федеральных Агентств. Идентификация информационных систем включает в себя идентификацию интерфейсов между системой, используемой в различных федеральных Агентствах и другими системами или сетями.

Вся информация и информационные системы должны быть классифицированы на основе целей обеспечения надлежащего уровня информационной безопасности в соответствии с диапазоном рисков.

Стандарт FIPS 199 "Standards for Security Categorization of Federal Information and Information Systems" определяет диапазоны безопасности.

Федеральные информационные системы должны соответствовать минимальным требованиям безопасности, определенным стандартом

[24] https://en.wikipedia.org/wiki/Information_Security_Automation_Program
[25] https://nvd.nist.gov/
[26] https://scap.nist.gov/

обязательной безопасности FIPS 2000 Minimum Security Requirements for Federal Information and Information Systems[27].

Сочетание требований, указанных в документах - FIPS 2000 и NIST Special Publication 800-53[28] - определяют основополагающий уровень безопасности для всех федеральных информационных систем.

При оценке рисков информационной безопасности федеральных Агентств проверяется совокупность элементов управления информационной безопасностью и определяется необходимость принятия дополнительных мер обеспечения информационной безопасности для защиты деятельности федеральных Агентств (в том числе в части защиты миссии, функции, образа, или репутации), активов федеральных Агентств, физических лиц, других организаций или государства в целом.

Федеральные Агентства должны разрабатывать политику в отношении процесса планирования системы информационной безопасности.

Законопроект **Domestic Security Enhancement Act of 2003** (Закон о повышении внутренней безопасности), называемый также **Patriot II Act** подготовлен Департаментом юстиции в 2003 году.

Предварительный вариант законопроекта расширял полномочия Федерального Правительства США, что подразумевало:

- отмену назначаемых судом запретов в отношении шпионажа полицейских агентств;
- предоставление права ФБР на проведение обысков и наблюдения без предварительного получения судебного приказа на основании данных разведки в зарубежных странах;
- создание ДНК-базы лиц, подозреваемых в терроризме;
- освобождение от гражданской ответственности предприятий и физических лиц, добровольно представивших Правительству личную информацию;
- криминализацию деятельности по шифрованию для сокрытия компрометирующих связей.

С точки зрения оценки стратегических подходов к обеспечению кибербезопасности, интерес также представляет **The 2011 U.S. Department of Defense Strategy for Operating in Cyberspace** (Стратегия операций в

[27] FIPS 2000 Minimum Security Requirements for Federal Information and Information Systems // http://csrc.nist.gov/publications/PubsFIPS.html

[28] http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

киберпространстве Министерства обороны США, 2011)[29]. (далее Стратегия 2011) Стратегия 2011 содержит оценку проблем и возможностей, возникающих в связи с ростом значения информационных технологий для военных, разведывательных операций и бизнеса. Стратегия 2011 является секретной, рассекреченный релиз раскрывает пять «Стратегических инициатив» Министерства обороны США в киберпространстве.

При этом основной акцент делается на стратегические преимущества киберпространства, включающие в себя оперативную связь и возможности обмена информацией и знаниями в сфере информационных технологий, в том числе осуществление экспертиз в сфере кибербезопасности. Дополнительный акцент делается на развитие международного сотрудничества США в киберпространстве в рамках международного взаимодействия, коллективной обороны, а также установление международных норм, регулирующих киберпространство. Стратегия 2011 раскрывает совокупность киберугроз, к которым относит в т.ч. доступность хакерских программ, способных при незначительных затратах ресурсов причинить непропорционально большой урон, что представляет значительную угрозу для национальной безопасности США.

Стратегией 2011 приводится анализ внешних и внутренних угроз, уязвимостей цепочек поставки и угроз для оперативной деятельности министерства обороны. Документ оценивает возникающие угрозы как сложные и критически важные для национальной и экономической безопасности.

В свете рисков и возможностей, возникающих у министерства обороны и администрации США при использовании киберпространства, документ содержит пять стратегических инициатив, реализация которых позволит эффективно действовать в киберпространстве, защищать национальные интересы, и обеспечивать интересы национальной безопасности.

Стратегическая инициатива № 1 заключается в возможности использовать киберпространство в качестве оперативного пространства, организовать его оснащение и тренировки персонала так, чтобы министерство обороны могло в полной мере воспользоваться потенциалом киберпространства. Инициатива

[29] U.S. Department of Defense, «Strategy for Operating in Cyberspace», July 2011 // [www.defense.gov/news/d20110714cyber.pdf

позволяет Пентагону организовать обучение и оснащение киберпространстве так же, как это делается в авиационных, наземных и морских частях, чтобы защищать интересы национальной безопасности. Реализация инициативы напрямую связана с деятельностью Кибернетического командования США как подразделения Стратегического командования США для координации киберкомандований родов войск. Кибернетическое командование США организационно совмещено с Агентством национальной безопасности, причем командующий Кибернетическим командованием занимает одновременно пост главы АНБ.

Стратегическая инициатива № 2 дает возможность применять новые концепции защиты для защиты компьютерных сетей и систем министерства обороны и включает использование лучших практик «кибергигиены», в т.ч. обновлённое программное обеспечение и совершенствование управления компьютерными сетями. Министерство обороны принимает меры по повышению квалификации кадров, улучшению отчётности, внутреннего контроля и возможностей управления информационными потоками для снижения уровня внутренних угроз, по активизации защиты, а также разработке новых концепций защиты сетей и вычислительных архитектур, включая мобильные СМИ и безопасные облачные вычисления, с целью своевременного обеспечения безопасности быстро меняющимся устройствам и приложениям.

Стратегическая инициатива № 3 включает в себя партнерство с другими американскими правительственными ведомствами и учреждениями и частным сектором в интересах общенациональной стратегии кибербезопасности. Особенность инициативы состоит в том, что важные функции министерства обороны зависят от бизнес-партнеров, включая интернет-провайдеров, что порождает риски, которые министерство обороны планирует снижать совместно с Министерством национальной.

С 2007 года в США действует программа **Defense Industrial Base Cyber Security and Information Assurance program** (Программа кибербезопасности и обеспечения сохранности информации в оборонной промышленности).

Стратегическая инициатива № 4 заключается в необходимости выстроить надежные отношения с союзниками США и другими международными

партнерами в целях усиления общей кибербезопасности», что включает разработку международных норм и принципов действий в киберпространстве, сдерживания вредоносных акторов и защиту жизненно важных национальных активов. Запланированные министерством мероприятия предполагают проведение совместного обучения специалистов, обмен передовым опытом и развитие механизмов сотрудничества.

Стратегическая инициатива № 5 предполагает увеличить изобретательность нации благодаря высокому профессионализму кадров и быстрым технологическим инновация, для чего использовать лучшие научные, академические и экономические ресурсы США для формирования корпуса квалифицированных кадров, как военных, так и гражданских, для работы в киберпространстве и достижения заявленных в доктрине целей. Министерство обороны США выдвигает пять принципов для реализации данной инициативы:

- скорость обработки данных является одним из важнейших приоритетов;
- рост разработки и тестирования программных продуктов;
- отсроченная кастомизация для постепенного улучшения;
- различные уровни надзора, основанные на приоритете критически важных систем;
- меры по повышению безопасности аппаратного и программного обеспечения.

Министерство обороны намерено использовать возможности бизнеса, и работать с предпринимателями в сфере развития инновационных технологий путем применения целевых инвестиций и создания совместных предприятий.

Министерство обороны также организовало через DARPA (Агентство по перспективным оборонным научно-исследовательским разработкам Министерства обороны США) проект **National Cyber Range**, целью которого является быстрое создание моделей компьютерных сетей военного назначения, предназначенных для тестирования имитационного моделирования новых технологий.

В 2005 году в США принята Федеральная программа **Networking and Information Technology Research and Development (NITRD)**30, на осуществление деятельности которой выделяется 2.5 миллиарда долларов ежегодно, объединяющая деятельность Федеральных агентств по следующим направлениям:

- Обработка Больших данных - Big Data (BD)
- Кибербезопасность и обеспечение сохранности информации (CSIA)
- Взаимодействие человека с компьютером и управление информацией (HCI & IM)
- Программное обеспечение и системы высокого уровня защиты (HCSS)
- Сети высоких разрядов (LSN)
- Дизайн программного обеспечения и производительности (SDP)
- Спектр исследований в сфере беспроводных сетей и их развития (WSRD)

Программа NITRD работает под эгидой подкомитета Национального научного и технологического совета (NSTC) Комитета по технологии, который включает представителей от каждого из агентств NITRD-членов и обеспечивает общую координацию для NITRD деятельности.

Финансирование программы NITRD из федерального бюджета направлено на обеспечение революционных прорывов в области передовых информационных технологий, таких как вычислительные, сетевые технологии и программное обеспечение.

Программа NITRD обеспечивает научные исследования и разработки, направленные на обеспечение технологического лидерства США в сфере разработки передовых сетей, вычислительных систем, программного обеспечения и связанных с ними информационными технологиями. Программа NITRD осуществляет научные исследования и разработки для удовлетворения потребностей федерального правительства для продвинутых сетей, вычислительных систем, программного обеспечения и связанных с информационными технологиями.

В рамках Программы NITRD осуществляется комплекс мер, направленных на ускорение разработки и внедрения технологий в целях: сохранения лидерства США в области науки и техники; укрепления национальной обороны и национальной безопасности; повышение конкурентоспособности

[30] The Federal Networking and Information Technology Research and Development Program: Funding Issues and Activities, Updated May 2, 2005 // Congressional Research Service / The Library of Congress

США и развитие долгосрочного экономического роста; улучшение здоровья граждан США; защиты окружающей среды; повышения уровня образования, подготовки и непрерывного обучения; а также улучшения качества жизни.
Межведомственная рабочая группа координирует деятельность компонентов программной области направления кибербезопасности и обеспечения сохранности информации (CSIA). Деятельность CSIA сосредоточена на исследованиях и разработках по предотвращению, выявлению, реагированию действий, ставящих угрозу доступность, целостности, конфиденциальность компьютерных и сетевых систем.

1.2. Национальные стратегии кибербезопасности в странах ЕС и НАТО

В начале XXI века стали появляться первые национальные стратегии кибербезопасности европейских стран. Начало процесса было положено с принятием в США National Strategy to Secure Cyberspace (2003)[31], выступавшей частью National Strategy for Homeland Security напрямую связанной с последствиями терактов 11 сентября 2001 года.
В 2005 году в Германии был принят National Plan for Information Infrastructure Protection (NPSI)[32].
В 2008 году Эстония, впервые среди членов Европейского союза, публикует национальную стратегию кибербезопасности[33].С указанного времени явлене приобретает лавинобразный характер, Стратегии принимаются большинством стран Евросоюза, причем в национальных стратегиях отражаются некоторые специфические особенности:
В 2006 году Швеция принимает Strategy to improve Internet security in Sweden.

Правительство Швеции поручило Agency for Civil Protection and Preparedness MSB (Агентство по защите населения и готовности) администрирование национального плана действий для обеспечения информационной безопасности, который был составлен в 2008 году и обновлен в 2010 году. План основывается на стратегии национальной

[31] *http://www.dhs.gov/files/publications/editorial_0329.shtm*
[32] *http://www.bmi.bund.de/cae/servlet/contentblob/560098/publicationFile/27811/kritis_3_eng.pdf*
[33] http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

безопасности информации и был создан в сотрудничестве с рядом других органов и организаций в этой области.

В качестве приоритетов определены четыре основные области:

- необходимость совершенствования многосекторальной и межсекторальной работы по социальной информации и безопасности. Всеобъемлющее правила информационной безопасности могут быть разработаны таким образом, чтобы применять их во все инстанции под контролем правительства;

- следует создать базовый уровень безопасности для безопасности общественной информации, что является предпосылкой для обеспечения информационными ресурсами, которые все чаще приобретают основополагающее значение для сектора торговли и общественного сектора;

- общество должно иметь возможность обрабатывать обширную информацию, связанную с ИТ беспорядками и кризисами. При этом должны быть установлены оперативные национальные координационные функции;

- существует недостаток экспертизы безопасности информации на всех уровнях общества.

Франция фокусируется на готовности информационных систем противостоять событиям в киберпространстве, которые могут поставить под угрозу доступность, целостность и конфиденциальность данных.

Французская национальная стратегия по обороне и безопасности информационных систем принята в феврале 2011 года[34]принимает во внимание тот факт, что угрозы в отношении информационных систем влияют на безопасность государственных органов, предприятий и граждан, в особенности во Франции.

Для достижения целей информационной безопасности определены 7 основных направлений:

- анализ окружающей обстановки для принятия надлежащих решений;

- обнаружение атак и противодействие им, предупреждение потенциальных жертв и помощь им;

- увеличение и усиление французского научного, технического, промышленного и человеческого потенциала для обеспечения необходимой автономии;

[34] *www.ssi.gouv.fr/site_article318.html*

- защита информационных систем государства и операторов жизненно важных объектов инфраструктуры, для совершенствования национальной устойчивости;
- адаптация права, с учетом эволюции в области технологий и новых видов применения;
- разработка Францией механизмов международного сотрудничества в области безопасности информационных систем, борьбе с кибер-преступностью и кибер-защиты, для того, чтобы лучше защитить национальные информационные системы;
- информирование и обучение населения для получения ими информации о безопасности информационных систем.

Национальная Стратегия подчеркивает значимость использования технических средств, направленных на обеспечение безопасности информационных систем, борьбу с киберпреступностью и создание кибероборонны[35].

В июле 2009 Правительством Франции создано ANSSI, the French Network and Information Security Agency.

В мае 2010 года Постановление о безопасности информсистем [36]было издано в целях исполнение Постановления об электронном взаимодействии между государственными пользователями услуг и органами государственной власти, - также известный как Постановление о телекоммуникационных услугах (**Ordinance on electronic interactions between public services users and public authorities and among public authorities - „teleservices ordinance**)- принято 8 декабря 2005 года на основе Legal Simplification Law от 9 декабря 2004 года. Оно направлено на создание всеобъемлющей правовой основы для перехода к «электронной администрации» к 2008 году, путем создания условий для простого и безопасного электронного взаимодействия между гражданами и государственными органами. Текст охватывает весь обмен электронными документами, электронную почту или цифровую связь между государственными органами (с одной стороны), а с другой стороны, гражданами и центральной администрацией, региональным правительством и частными организациями. Он дает такой же правовой статус к электронной почте, как и у традиционным бумажным письмам и

[35] http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011
[36] Referential on the security of information systems (RGS) // *www.ssi.gouv.fr/rgs*

легализует использование электронной подписи органами государственной власти. Кроме того, постановление включает в себя обеспечение для пользователей, чтобы имели возможность безопасного хранения и получения официальной корреспонденции и административных форм на личных интернет-почтовых ящиках. Наконец, текст устанавливает положения о безопасности обменов и взаимодействия информационных систем.

Национальная стратегия Германии German National Strategy for Critical Infrastructure Protection (CIP Strategy) опубликована в июне 2009 года - **Bundesministerium des Innern** (BMI), обобщает цели, подход и практику применения,[37] в т.ч. включает Национальный план защиты инфраструктуры в области ИКТNational Plan for Infrastructure Protection (NPSI)

Для реализации указанной Стратегии предлагает использование ряда инструментов, включающих в себя:

- программы и соответствующие планы осуществления стратегической деятельности для защиты ИТ-инфраструктуры);

- конкретные рекомендации, например: Национальная концепция основных мер защиты, Базовое руководство по физической защите важнейших объектов инфраструктуры;

- характеристики рисков и управления в кризисных ситуациях критических операторов инфраструктуры, национальные специальные понятия защиты, такие как подробные рекомендации для принятия мер по защите отдельных секторах CI и суб-секторов;

- стандарты, нормы и правила;

В начале 2011 года в Германии принята новая Федеральная стратегия кибербезопасности Германии - (Federal Cyber Security Strategy for Germany)[38], в которой выделены следующие основные направления обеспечения кибербезопасности:

Основным приоритетом кибербезопасности является защита критических информационных структур и обеспечение сотрудничества определеяемое планом CIP;

Безопасность ИТ в Германии осуществляется на основании совместной деятельности общества и государства строящейся на соотнесении угроз и

[37] *http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf*
[38] http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Sicherheit/css_engl_download.pdf?__blob=publicationFile

мер, при этом комплекс инструментов защиты должен быть значительно расширен;

Укрепление ИБ в органах государственного управления строится на общной, единообразной и безопасной сетевой инфраструктуры федеральной администрации, использующейся в качестве основы и передачи данных4

Национальный центр кибер - реагирования (National Cyber Response Centre) оптимизирует оперативное сотрудничество между всеми органами государственной власти и улучшение координации мер защиты и реагирования на ИТ-инциденты;

Национальный совет кибер-безопасности (National Cyber Security Council) намерен координировать превентивные инструменты и междисциплинарные подходы кибер-безопасности в государственном и частном секторе, выступая дополнительным и связующим звеном ИТ-управления на федеральном уровне, с участием различных министерств и федеральных органов;

Эффективный контроль за преступностью в киберпространстве включает в себя комплекс совместных институтов с участием предпринимателей и компетентных правоохранительных органов для разработки рекомендаций. Значительный результат в сфере достижения глобальной гармонизации в области уголовного права на ожидается на основе Конвенции Совета Европы о киберпреступности;

В сфере внешней политики Германия намерена согласованно и последовательно отстаивать свои интересы в международных организациях;

Германия будет продолжать и активизировать исследования по ИТ-безопасности и защите важнейших объектов инфраструктуры, направленные на укрепление своего технологического суверенитета и экономического потенциала во всем диапазоне основных стратегических ИТ-компетенций.

Стратегия устанавливает основу для защиты критически важных информационных структур, исследует существующие нормативные акты для выявления дополнительных полномочий в сфере обеспечения информационных технологий в Германии посредством предоставления основных функций безопасности, сертифицированных государством[39].

[39] http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1

Стратегия Великобритании (2011) заявляет цель в защите от кибератак со стороны преступников, террористов и враждебных государств, угроз и рисков в данной сфере, обеспечение безопасности для граждан и бизнеса[40].

18 октября 2010 года в Великобритании принята **Национальная стратегия безопасности,** а в ноябре 2011 года в Великобритании принята **The UK Cyber Security Strategy**, предусматривающая ежегодное вложение 650 млн. фунтов до 2015 года на реализацию National Cyber Security Programme (NCSP). приоритетными направлениями деятельности данной Стратегии являются:

- обнаружение и анализ сложных электронных угроз;
- разработка международных принципов или «правил дорожного движения» за поведение в киберпространстве;
- участие в интеграционных процессах по совершенствованию национального уголовного законодательства стран – участниц Будапештской конвенции о киберпреступности, с целью убеждения других стран в необходимости разработки соглашений о привлечении к ответственности через границы за совершение кибер-преступлений и об отказе в предоставлении убежища кибер-преступникам;
- поддержка эффективной правовой основы и правоприменительные возможности преследования кибер-преступности, упрощая сообщения о преступлениях и процедуру реакции на них;
- установление высоких стандартов для поставщиков государственных киберуслуг;
- содействие развитию кадров квалифицированных специалистов по кибер - безопасности;
- повышение осведомленности и просвещения людей и фирм, чтобы защитить себя в Интернете;
- создание в киберпространстве рынка продукции и услуг;
- осуществление интеграционных процессов в сфере «дальнейшего развития возможностей по предупреждению, выявлению, защитите от кибер-атак, в том числе с помощью НАТО, осуществление централизованной кибер защиты и лучшей интеграции в НАТО» в связи резолюцией Лиссабонского

[40] http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

саммита НАТО 04 июня 2010 года, подчеркнувшей значимость киберобласти как области значительных новых рисков и возможностей для Альянса.

В рамках указанных целей в Великобритании осуществляется деятельность по следующим направлениям:

- создание потенциала сдерживания и защиты от угроз высокого уровня;
- осуществление деятельности по международному сотрудничеству в киберпростанстве;
- снижение уязвимости правительственных систем и критических технологий, в т.ч. в рамках Cloud Computing Strategy [41]; и партнерство по программе «hub», предполагающей совместную деятельность правительства и деловых кругов;
- поощрение профессиональных кадров в области кибербезопасности;
- развитие системы борьбы с киберпреступностью;
- профилактика и информирование общественности;
- повышение осведомленности бизнеса;
- содействие бизнес- возможностям.

Стратегия Эстонии (2008) подчеркивает необходимость безопасного киберпространства в целом и фокусируется на информационных системах. В основу Стратегии положены меры гражданского характера, рекомендовано сосредоточить усилия на регулировании, образовании и сотрудничестве.

Стратегия Финляндии (2008) рассматривает кибербезопасность как вопрос безопасности данных, независимо от экономической значимости информации в свете развития финского информационного общества[42].

Словакия (2008) рассматривает обеспечение информационной безопасности как важный компонент развития и функционирования общества, в связи с чем цель Стратегии состоит в разработке всеобъемлющего обеспечения и на профилактику противоправной деятельности.

Основные цели Стратегии кибербезопасности Чехии (2011) включают защиту от угроз, которым подвергаются информационно-коммуникационные системы и технологии, а также смягчение возможных последствий в случае нападения на ИКТ. Стратегия ориентирована в основном на беспрепятственный доступ к услугам, целостность данных и

[41] http://www.cabinetoffice.gov.uk/sites/default/files/ resource /government-cloud-strategy_0.pdf

[42]

конфиденциальность. Киберпространство и республики координируется с другими соответствующими стратегиями и концепциями[43].

Кроме стран Евросоза, в указанный период времени Стратегии принимаются и другими странами.

Стратегия кибербезопасности Канады (2010) строится на принципах обеспечения безопасности государственных систем, партнерства для обеспечения жизненно важных киберсистем за пределами федерального правительства и обеспечение безопасности канадцев в Интернете. Первый компонент Стратегии направлен на установление четких функций и обязанностей в целях укрепления безопасности федеральных киберсистем и повышения уровня информированности о кибербезопасности в правительстве. Второй компонент охватывает целый ряд партнерских инициатив провинций и территорий с участием частного сектора и важнейших секторов инфраструктуры. И, наконец, третий компонент охватывает борьбу с киберпреступностью и защиту канадских граждан в Интернете[44].

Стратегия кибербезопасности Японии (2010) включает в себя ряд положений, связанных с усилением политики с учетом возможных кибератак и определяет необходимость создания реагирующих организаций, возможность адаптации к изменениям в окружающей среде информационной безопасности, а также установление активных, а не пассивных мер по обеспечению информационной безопасности[45]. При этом в качестве основных направлений деятельности предлагаются:

- преодоление ИТ-рисков для реализации кибербезопасности;
- осуществление политики, усиливающей национальную безопасность и кризисное управление в области ИКТ как основы социально-экономической деятельности;
- созданием политики информационной безопасности, которая вносит свой вклад в стратегию экономического роста;
- формирование международных альянсов.

[43] http://www.enisa.europa.eu/media/newsitems/CZ_Cyber_Security_Strategy_20112015.PDF
[44] *http://publications.gc.ca/site/eng/379746/publication.html*
[45] *http://www.nisc.go.jp/eng/*

При этом, согласно исследованию European Union Agency for Network and Information Security (ENISA)[46] основными характеристиками национальных Стратегий кибербезопасности выступают:

- определение сферы кибербезопасности;
- определение механизмов государственно-частного партнерства, позволяющего всем заинтересованным сторонам участвовать в обсуждении и согласовании политических и нормативных решений в сфере кибербезопасности;
- определение необходимых политических и нормативных мер, прав и обязанностей государственных органов и предприятий частного сектора, включая новые правовые рамки борьбы с киберпрестпностью, обязательную отчетность об инцидентах, минимальные меры безопасности и руководящие принципы;
- участие в международной деятельности по борьбе с киберпреступностью;
- выявление важнейших информационных инфраструктур, включая ключевые активы и услуги;
- разработка мероприятий по защите;
- определение системного и комплексного подхода к национальному управлению рисками;
- международное сотрудничество.

При разработке Стратегии интернет-безопасности Европейского Союза определен ряд целей[47]:

- описание основных проблем и рисков;
- анализ экономических и политических возможностей;
- проведение оценки текущих или запланированных действий, а также выделение областей, где существует наибольшая необходимость привлечения ЕС;
- составление карты проблем (картирование)[48].

При этом, заявленными критериями картирования национальных Стратегий кибербезопасности (NCSS) выступают[49]:

[46] National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace // ENISA/ 2012/15 p
[47] http://ec.europa.eu/atwork/programmes/docs/cwp2012_en.pdf
[48] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map
[49] An evaluation Framework for National Cyber Security Strategies. European Union Agency for Network and Information Security. 2914// www.enisa.europa.eu

- развитие и внедрение законодательной базы;
- определение уровня сотрудничества между государственным и частным сектором;
- уточнение значения инвестиций в ИКТ в целях обеспечения кибербезопасности и неприкосновенности частной жизни;
- защита и эффективное функционирование критической информационной инфраструктуры;
- обеспечение открытого, стабильного и безопасного киберпространства;
- осознание гражданами достаточной защищенности данных;
- защита цифровых национальных информационных ресурсов;
- образование и профессиональная подготовка;
- международная позиция государственных органов;
- закрепление жизненно важных национальных интересов от кибератак и угроз;
- обеспечения готовности, устойчивости и адекватного реагирования на киберугрозы и нападения;
- степень зависимости экономики от уровня информатизации;
- повышение осведомленности;
- борьба с киберпреступностью;
- соблюдение установленных правил в соответствии с национальным нормами;
- безопасное использование информации и ИКТ государственными органами, гражданами и бизнесом;
- безопасность ведения бизнеса;
- качество информационных технологий и коммуникационных продуктов и стандарты безопасности;
-безопасное киберпространство в отношении основных прав и ценностей.

Некоторые цели определены значительным количеством стран, некоторые из них относятся к одной стране или группе стран. Так, борьба с киберпреступностью характерна для Стратегий Нидерландов и Великобритании, защита и эффективное функционирование критической информационной инфраструктуры характерны Стратегиям Франции, Румынии, Бельгии и др.

Частные цели служат для определения фокусных направлений и выделяют конкретные участки координации деятельности государственных органов, коммерческих организаций, научного сообщества и других заинтересованных сторон, включающие в себя:

- разработку стандартов и норм законодательства;
- деятельность по укреплению стратегического и международного сотрудничества;
- создание культуры безопасности путем информирования, обучения и повышения уровня осведомленности;
- осуществление исследований, разработок и инноваций;
- гарантия безопасности услуг, предоставляемых в киберпространстве;
- поддержка компетентности и потенциала вовлеченных сторон;
- отслеживание угроз, рисков и реагирования.

Для определения совокупности финансовых, людских и технологических ресурсов используется совокупность входных и выходных индикаторов. Индикаторы входа указывают на ресурсы, которые доступны для реализации NCSS на обеих уровнях конкретных целей NCSS и включают:

- законодательные меры;
- использование правоохранительных и судебных возможностей;
- участие в международном и региональном сотрудничестве;
- создание (улучшение) процессов и координационных структур;
- исследования и разработки поддержки;
- осуществление исследований по отдельным государственным и частным компонентам сети;
- стимулирование и финансирование инициатив, поддерживающих безопасные системы.

Критериями выхода выступают непосредственные результаты программных мероприятий, которые могут быть проконтролированы и относительно легко измерены количественно и качественно. Критерии выхода также служат в качестве входных критериев для последующих этапов и включают в себя:

- годовые отчеты;
- минимальные стандарты кибербезопасности;
- улучшение нормативно-правовой базы;

- разработку процессов, инструментов и координирующих структур, а также планов реагирования на чрезвычайные ситуации;
- международное сотрудничество;
- научные исследования и разработки (фактические инвестиции);
- возможности для борьбы с киберпреступностью;
- разработку систем предупреждения;
- соблюдение гражданских прав человека в киберпространстве;

Результаты отражают краткосрочные и среднесрочные результаты программы, в то время как последствия характеризуют последствия, наступающие с более чем десятилетним сроком, расположенные, как правило, в контексте с целями и областями действия.

Команды реагирования на чрезвычайные компьютерные ситуации (Computer Emergency Response Teams – CERTs) играют жизненно важную роль в процессе оценки критических ситуаций. Команда отвечает за измерение информационной безопасности, ведет оценку кибербезопасности, публикующуюся несколько раз в год. CERT осуществляют анализ ключевых индикаторов, таких как количество уязвимостей, инфекций вредоносных программ и разработок, наличие инцидентов в сфере безопасности.

Фактор защиты критической инфраструктуры (Critical Infrastructure Protection, CIP) связан с отсутствием прямого государственного контроля в большинстве государств-членов над критической инфраструктуры отрасли, так как значительная часть инфраструктуры находятся в руках частных компаний. В ряде государств деятельность CIP рассматривается отдельным направлением, в других государствах-членах, CIP является ключевым направлением деятельности национальной Стратегии.

Ключевые показатели эффективности (Key Performance Indicators, KPI) являются важными критериями, которые могут используются для измерения уровня исполнения национальных стратегий NCSS. Используемые при этом ключи-индикаторы отображают процесс планирования и оценки с использованием матрицы характеристик.

Разработка политики и возможности киберзащиты (ключевая цель 1) может быть достигнута после реализации национальной Стратегии.

Достижение кибер-устойчивости (ключевая цель 2) заключается в развитии потенциала эффективного сотрудничества государственного и частного сектора.

Сокращение киберпреступности (ключевая цель 3) содержит набор ключевых показателей для измерения деятельности по сокращению киберпреступности на национальном и международном уровнях.

Разработка промышленных и технологических ресурсов для кибербезопасности (ключевая цель 4) напрямую связана с необходимостью поддержки надлежащего уровня кибербезопасности на рынке продуктов.

Безопасная критическая информационная инфраструктура (ключевая цель 5) включает в себя информацию об инцидентах, идентификацию критических инфраструктур, международное сотрудничество.

При этом к числу недостатков национальных стратегий кибербезопасности с стран-участников ЕС, можно отнести:

- отсутствие конкретных планов действий в рамках стратегии, четкого указания масштаба и целей стратегий, а также конкретного определения кибербезопасности;
- отсутствие четких рекомендаций для правительственных ведомств, национальных органов власти и других государственных органов;
- отсутствие согласованности с промышленными предприятиями, научными кругами и представителями гражданского общества;
- отсутствие сотрудничества с другими государствами и Европейской комиссией для обеспечения трансграничного и глобального характера кибербезопасности;
- отсутствие возможности по учету новых рисков, а также улучшения и расширения использования информационных и коммуникационных технологий;
- возможность конфликта национальных стратегий кибербезопасности с целями международного сообщества.

В настоящее время представляет интерес предложение по **Directive of the European Parliament and of the council concerning measures to ensure a high common level of network and information security across the Union**

(Директиве обеспечения информационной безопасности на территории ЕС)[50], представленный Европейской комиссией в феврале 2013 года.

Директива определяет основной целью гармонизацию подходов к информационной безопасности в государствах–членах ЕС. Директива содержит требования к частным компаниям о представлении информации об инцидентах в области информационной безопасности. К числу компаний отнесены операторы критической инфраструктуры в области энергетики, транспорта, финансовой отрасли, здравоохранения компании, осуществляющие интернет-услуги. Приложение 2 Директивы включает в круг регулируемых субъектов операторов объектов критической инфраструктуры, организации, деятельность которых в ЕС определяется термином «услуги информационного общества»:

- платформы электронной коммерции;
- компании, обеспечивающие доступ к системам интернет-платежей;
- социальные сети;
- поисковые системы;
- компании, работающие в сфере облачных вычислений;
- магазины программ-приложений.

В октябре 2014 года, когда проект директивы находился на рассмотрении Совета ЕС, в проект Директивы были включены точки обмена интернет-трафиком, регистраторы доменных имен и компании, предоставляющие услуги веб- хостинга.

Директивой определено понятие безопасности как способность сети и информационной системы противостоять (при заданном уровне доверия) авариям или действиям злоумышленников, ставящим под угрозу доступность, подлинность, целостность и конфиденциальность хранимых или передаваемых данных или связанных с ними услуг, предлагаемых или доступных через эту сеть или информационную систему. Под риском понимается любое обстоятельство или событие, имеющее потенциальное негативное влияние на безопасность; инцидент означает любое

[50] Directive of the European Parliament and of the council concerning measures to ensure a high common level of network and information security across the Union // Brussels, 7.2.2013 COM(2013) 48 final 2013/0027 (COD) Proposal for a {SWD(2013) 31 final} {SWD(2013) 32 final} // http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

обстоятельство или событие, имеющее фактическое неблагоприятное воздействие на безопасность.

При этом каждое государство принимает национальную стратегию NIS для определения стратегических целей, конкретной политики и регулирующие меры для достижения и поддержания высокого уровня сетевой и информационной безопасности.

Каждое государство назначает национальный компетентный орган по безопасности сетевых и информационных систем ("компетентный орган"), деятельность которого направлена на контроль за исполнением Директивы на национальном уровне и вносит вклад в его последовательное применение на всей территории Евросоюза.

Каждое государство создает Computer Emergency Response (CERT), несущую ответственность за обработку инцидентов и рисков в соответствии с четко определенным процессом.

Таким образом, в настоящее время в странах Евросоюза подготовлена почва для принятия Директивы об обеспечении информационной безопасности в киберпространстве, причем решение проблемы будет реализовываться с активным участием коммерческих организаций, осуществляющих свою деятельность в сфере ИКТ.

При этом представляется проблемным принципиальный выбор между государством и компаниями IT-индустрии: добровольное сотрудничество или регулирование в форме прямого государственного вмешательства с наложением обязательств и последующими санкциями, а также гармонизации этих подходов на глобальном уровне[51].

В 2009 году Директором Агентства НАТО по стандартизации НАТО утверждена Allied Joint Doctrine For Information Operations, AJP-3.10 (Союзническая информационная доктрина информационных операций, Доктрина)[52]. Доктрина определяет, что наблюдается смещение акцентов от несомненных сверхмощных противостояний в сторону более сложных взаимодействий государственных и негосударственных субъектов, связанное с глобализацией, конкуренцией за ресурсы и напряженностью политических и социальных структур в сочетании с идеологическими, религиозными и

[51] Татьяна Тропина // http://www.pircenter.org/media/content/files/13/14412005930.pdf

[52] Allied Joint Doctrine For Information Operations, AJP-3.10, NATO, November 2009 // https://info.publicintelligence.net/NATO-IO.pdf

культурными различиями. Терроризм, наряду с распространением оружия массового уничтожения, скорее всего, останутся главными угрозами. Одновременно с этим, наблюдается «информационная революция» (Интернет и мобильные телефоны), что открыто эпоху компьютерного процесса принятия решений. Развитие информационной среды включает информацию, участников и системы, которые позволяют ее использовать. К участникам относятся руководители и лица, принимающих решения. Информационные системы включают материалы и системы, используемые для сбора, применения или распространения информации. Информационная среда (как основная среда принятия решений) включает в себя сферу, где люди и автоматизированные системы имеют возможность наблюдать, ориентировать, принимать решения и действовать на основе информации. НАТО находится в процессе разработки концепций, процессов и доктрины, в том числе информационных операций (Info OPS), чтобы отвечать новым вызовам.

Все кризисы происходят в центре внимания международных средств массовой информации. Влияние средств массовой информации увеличилось, что следует связывать с развитием технологий, таких как спутниковое вещание и подключение к глобальной сети Интернет. Кроме того, наличие относительно дешевой печатной и копировальной техники привнес газеты и другие печатные материалы для более широкой аудитории.

Информационная деятельность направлена конкретно на волю и сознание лиц, принимающих решения и обладающих возможностями. Эффекты в информационной среде могут быть созданы с помощью различных военных действий, тесная координация которых будет способствовать достижению общей цели. Доктрина включает в себя три взаимосвязанных направления деятельности:

- информационная деятельность, направленная на изменение восприятия противников;
- информационная деятельность, направленная на сохранение и защиту свободу маневра НАТО в информационной среде, защиту данных и информацию, поддерживающую лиц, принимающих решения и процессы принятия решений;

- информационные мероприятия, направленные на противодействие командным функциям и возможностям путем воздействия на данные и информацию, которые поддерживают противников и используются в управления и контроля, разведки, наблюдения и целеуказания, а также системы вооружения.

К принципам информационных операций Доктрина относит:

-основанный на воздействии подход к операциям;

- планирование и личное участие командования;

- тесная координация и секвестирование;

- использование точной информации;

- централизованное планирование и децентрализованное выполнение;

- совместное целеуказание;

- своевременность подготовки;

- непрерывность;

- мониторинг и оценка.

Целью информационной безопасности является защита информации в процессе хранения, обработки или передачи, а также хост-системы, от потери конфиденциальности, целостности и доступности в системах процедурных, технических и административного контроля. Информационная безопасность осуществляет комплекс мероприятий для обеспечения защиты информации и является неотъемлемой частью всех военных операций и включает:

- Communications Security (безопасность коммуникаций, COMSEC);

- Computer Security (компьютерную безопасность, COMPUSEC),

- Computer Network Defence (компьютерные сети обороны, CND), как интегрированную часть Computer Network Operations (компьютерные сетевые операции, CNO), совместно с персоналом, документооборотом, физической и процедурной безопасностью.

Компьютерные Сетевые Операции. Состоят из 3 интегрированных элементов:

- Computer Network Attack (Компьютерные Сетевые атаки, CNA) а основанные на том, что программные и аппаратные уязвимости компьютеров, устройств хранения и сетевого оборудования позволяют атаковать путем использования вредоносного кода, вирусов или тонких манипуляций с компьютерными данным, что напрямую связано с

увеличением объема коммерческого программного обеспечения в системах военного назначения;

- Computer Network Exploitation (Эксплуатацию компьютерной сети, CNE) напрямую связано с возможностью получать сведения о компьютерах и компьютерных сетях;

- Computer Network Defence (Оборона компьютерной сети, CND) заключается в защите от атак (CNA) и эксплуатации (CNE) и представляет собой меры защиты от разрушения, деградации или уничтожение данных в компьютерах или сетях. CND имеет важное значение для поддержания процесса принятия решений.

Контекст выбора соответствующих информационных мероприятий, предусмотренных Доктриной, представлен на рис.1.

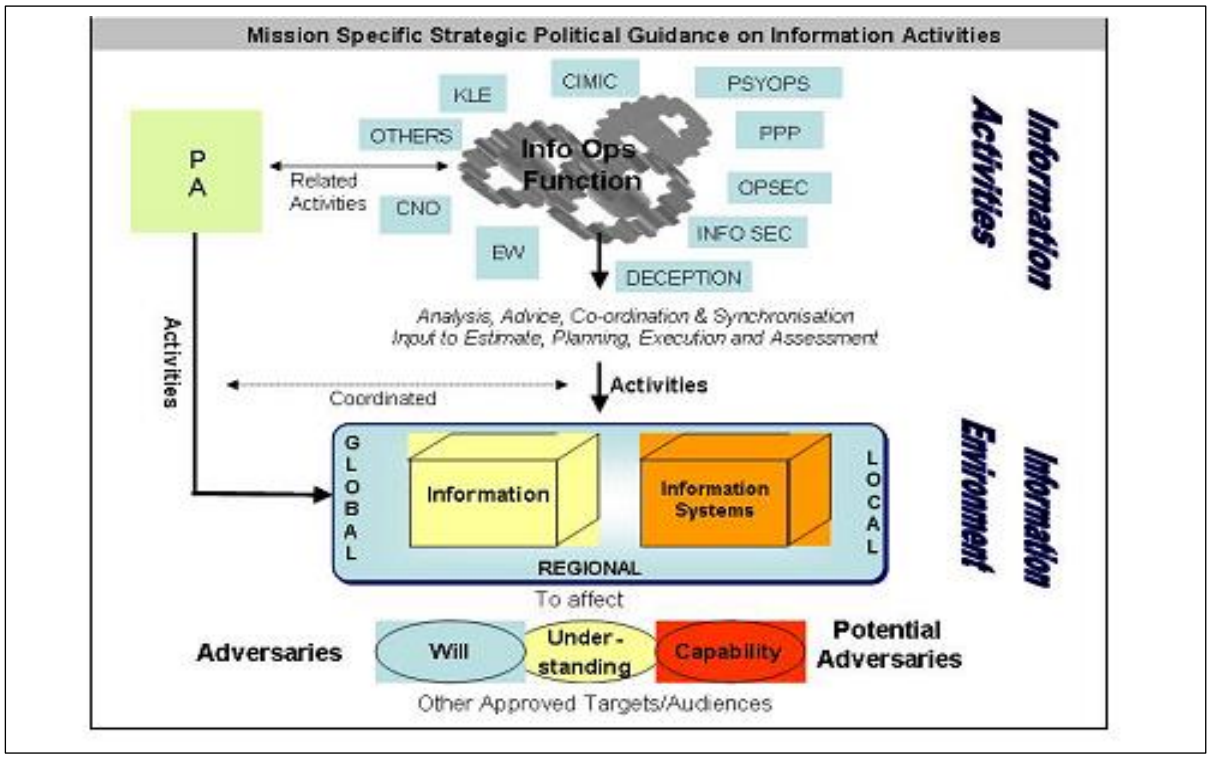

Рис. 1. Совокупная характеристика подхода Доктрины.

Таким образом, существующие в настоящее время Национальные Стратегии кибербезопасности представляют интерес, в первую очередь, с точки зрения определения киберпространства как сферы правового регулирования, что подразумевает складывающиеся отношения в сфере практики использования электронного документа в деятельности государственных и коммерческих организаций, определение практической значимости и финансовой

ценности компьютерной информации, сложившуюся методику борьбы с преступлениями в данной сфере. Согласованная деятельность в данной сфере позволяет сделать вывод о том, что в странах Евросоюза принято решение о выделении из совокупности правоотношений информационной безопасности, - правоотношений в сфере компьютерной (кибер-) безопасности.

Практически одномоментные разработка и принятие странами Евросоюза национальных Стратегий кибербезопасности может свидетельствовать о необходимости решения назревшей проблемы. В настоящее время принятие согласованного решения несколько затормозилось, не в последнюю очередь из-за невозможности распределения правомочий и обязанностей между участниками кибер-правоотношений. При этом в ряде стран (Франция, Германия) приняты новые редакции стратегий кибербезопасности.

1.3. Стратегия формирования правовых методов информационной безопасности Российской Федерации

В утвержденной Указом Президента РФ № 683 от 31 декабря 2015 г. Стратегии национальной безопасности Российской Федерации[53] определено, что информационную безопасность, как и безопасность личности следует прежде всего относить в число видов безопасности, структурно составляющих национальную безопасность.

При этом противоправная деятельность, связанная с использованием информационных и коммуникационных технологий, отнесена к числу основных угроз государственной и общественной безопасности. Указанное обстоятельство связывается со стремлением ряда стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, усилением противоборства в глобальном информационном пространстве, появлением новых форм противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий. В связи с изложенным при реализации Стратегии особое внимание уделяется обеспечению

[53] Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» //СЗ РФ ", 04.01.2016, № 1 (часть II), ст. 212

информационной безопасности с учетом стратегических национальных приоритетов.

Документом стратегического планирования государственной политики Российской Федерации в области международной информационной безопасности[54] определен перечень основных угроз использования информационных и коммуникационных технологий:

- в качестве информационного оружия;
- в террористических целях;
- для вмешательства во внутренние дела суверенных государств;
- для совершения преступлений.

Исходя из комплекса угроз, определены основные направления государственной политики Российской Федерации, связанной с решением круга задач:

- по формированию системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях;
- по созданию условий, способствующих снижению риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;
- по формированию механизмов международного сотрудничества в области противодействия угрозам использования информационных и коммуникационных технологий в террористических целях;
- по созданию условий для противодействия угрозам использования информационных и коммуникационных технологий в экстремистских целях, в том числе в целях вмешательства во внутренние дела суверенных государств;
- по повышению эффективности международного сотрудничества в области противодействия преступности в сфере использования информационных и коммуникационных технологий;

[54] "Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года" (утв. Президентом РФ 24.07.2013 № Пр-1753) //СПС Консультант плюс

- по созданию условий для обеспечения технологического суверенитета государств в области информационных и коммуникационных технологий и преодоления информационного неравенства между развитыми и развивающимися странами.

Утвержденная Президентом Российской Федерации 7 февраля 2008 г. Стратегия развития информационного общества в Российской Федерации ставит задачу «обеспечения национальной безопасности в информационной сфере»[55]. Стратегия предусматривает меры противодействия использованию потенциала информационных и телекоммуникационных технологий в целях угрозы национальным интересам России, к числу которых относят:

- обеспечение безопасности функционирования информационно-телекоммуникационной инфраструктуры;
- обеспечение безопасности функционирования информационных и телекоммуникационных систем ключевых объектов инфраструктуры РФ, в том числе критических объектов и объектов повышенной опасности;
- повышение уровня защищенности корпоративных и индивидуальных информационных систем; создание единой системы информационно-телекоммуникационного обеспечения нужд государственного управления, обороны страны, национальной безопасности и правопорядка;
- совершенствование правоприменительной практики в области противодействия угрозам использования информационных и телекоммуникационных технологий во враждебных целях;
- обеспечение неприкосновенности частной жизни, личной и семейной тайны, соблюдение требований по обеспечению безопасности информации ограниченного доступа.

Положениями «Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года»[56] определен ряд мер долгосрочного характера направленных на обеспечение информационной безопасности не только государственных органов власти, но и других организаций и граждан, проживающих на территории России:

[55] "Стратегия развития информационного общества в Российской Федерации" (утв. Президентом РФ 07.02.2008 № Пр-212) // РГ, № 34, 16.02.2008

[56] Распоряжение Правительства РФ от 01.11.2013 № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года» // СЗ РФ от 18.11.2013, № 46, ст. 5954.

- ускоренное развитие производства отечественной продукции гражданского назначения в целях формирования задела по самым перспективным направлениям развития отрасли информационных технологий;

- разработка и запуск специальной программы импортозамещения продукции сферы информационных технологий для решения задач отдельных государственных структур и организаций (в том числе оборонно-промышленного комплекса), включающей запуск разработки широкой номенклатуры продукции, обладающей высоким уровнем информационной безопасности;

- запуск в интересах отдельных государственных структур и организаций (в том числе оборонно-промышленного комплекса) специальной программы долгосрочных исследований для формирования научно-технического задела по информационным технологиям в соответствующих сферах с обеспечением максимально выгодного для государства перетекания технологий из гражданской в оборонную сферу и сферу двойных технологий и наоборот;

- стимулирование циркуляции данных "облачных" сервисов внутри страны;

- обеспечение стабильности развития отечественной отрасли информационных технологий и ее суверенности в долгосрочной перспективе за счет создания условий для развития в стране глобальных лидеров.

При всей значимости указанных программных документов следует иметь в виду их общий характер, возможность их использования исключительно для подготовки и уточнения доктринальных, концептуальных, программных и иных документов, определяющих цели и направления деятельности органов государственной власти, а также принципы и механизмы их взаимодействия с организациями и гражданами в области развития информационного общества в Российской Федерации.

17 апреля 2008 года Президентом Российской Федерации подписан Указ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных

сетей международного информационного обмена»[57], регламентирующий механизм обеспечения информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей, позволяющих осуществлять передачу информации через государственную границу Российской Федерации. Действие настоящего Указа в первую очередь направлено на совершенствование механизма защиты информации, составляющей государственную тайну.

До настоящего времени основным концептуальным документом, определяющим политику Российской Федерации в информационной сфере, содержание национальных интересов и потребность государства в обеспечении их безопасности, являлась Доктрина информационной безопасности Российской Федерации (далее: «Доктрина 2000»), одобренная на заседании Совета Безопасности Российской Федерации 23 июня 2000 года[58]. Доктрина утратила силу на основании Указа Президента Российской Федерации от 5 декабря 2016 года № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[59].

Доктрина 2000 подготовлена Советом Безопасности Российской Федерации и на нее наложена резолюция «Утверждаю» Президента Российской Федерации, в связи с чем можно полагать соответствие Доктрины категориям «декларация» или «программа».

Доктрина относила правовые методы к числу общих методов обеспечения информационной безопасности.

Необходимость разработки и принятия указанной Доктрины определялась рядом обстоятельств[60]:

- в условиях реализации конституционных прав граждан на свободу экономической, информационной и интеллектуальной деятельности[61]

[57] Указ Президента Российской Федерации от 17.04.2008. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» // СЗ РФ, 24.03.2008, № 12, ст. 1110.

[58] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // // РГ, № 187, 28.09.2000.

[59] Указ Президента Российской Федерации от 5 декабря 2016 года № 646 «Об утверждении доктрины информационной безопасности Российской Федерации» // http://kremlin.ru/acts/news/53418

[60] Емельянов Г.В., Стрельцов А.А. О Доктрине информационной безопасности Российской Федерации // http://emag.iis.ru/arc/infosoc/emag.nsf/f0c3e40261f64c5b432567c80065e37d/1894feb456dd29aec32569e700330026?OpenDocument.

[61] Жарова А.К. Правовая защита интеллектуальной собственности: учебное пособие. - М., 2011. - 248 с.

существенно увеличиваются потребности социально активной части общества в расширении информационного взаимодействия как внутри страны, так и с внешним миром;

- интенсивное развитие информационной инфраструктуры, и прежде всего информационно-телекоммуникационных систем, средств и систем связи, интеграция в мировое информационное пространство, а также информатизация практически всех сторон общественной жизни, деятельности органов государственной власти и управления существенно усилили зависимость эффективности функционирования общества и государства от состояния информационной сферы;

- индустрия информатизации, телекоммуникации и связи, информационных услуг на современном этапе развития человечества является одной из наиболее динамично развивающихся сфер мировой экономики, способной конкурировать по доходности с топливно-энергетическим комплексом, автомобилестроением, производством сельскохозяйственной продукции и определяющей наукоемкость промышленной продукции, ее конкурентоспособность на мировом рынке;

- информационная инфраструктура, информационные ресурсы во все большей степени становятся ареной межгосударственной борьбы за мировое лидерство; достижение противоборствующими странами определенных стратегических и тактических политических целей с учетом возрастающей зависимости российского общества от устойчивого функционирования информационной инфраструктуры, обеспечение безопасности интересов Российской Федерации в этой сфере становятся важным фактором национальной безопасности;

- индивидуальное, групповое и массовое сознание людей все в большей степени зависят от деятельности средств массовой информации и массовых коммуникаций.

Несмотря на то обстоятельство, что в настоящее время правовая основа Доктрины 2000 в значительной мере устарела, поскольку утратили силу стратегические документы и Федеральные законы, регулировавшие отношения в области обеспечения безопасности Российской Федерации на момент утверждения Доктрины, кардинально изменилась международная

обстановка, обращает на себя внимание то обстоятельство, что значительное количество положений Доктрины 2000 по-прежнему сохраняли свою актуальность:

- недостаточность нормативно-правового регулирования отношений в области реализации возможностей конституционных ограничений свободы массовой информации;
- несовершенное нормативное правовое регулирование отношений в области массовой информации, что затрудняет формирование на территории Российской Федерации конкурентоспособных российских информационных агентств и средств массовой информации;
- необеспеченность прав граждан на доступ к информации, манипулирование информацией, что вызывает негативную реакцию населения и в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе;
- практически не имеют достаточного обеспечения закрепленные в Конституции Российской Федерации права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки;
- неудовлетворительно организована защита собираемых федеральными органами данных о физических лицах (персональных данных);
- недостаточная четкость при проведении государственной политики в области формирования российского информационного пространства, а также в сфере развития системы массовой информации, организации международного информационного обмена и интеграции информационного пространства России в мировое информационное пространство;
- ухудшается ситуация с обеспечением сохранности сведений, составляющих государственную тайну;
- серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов;
- отставание отечественных информационных технологий вынуждает идти по пути закупок импортной техники и привлечения иностранных фирм при создании информационных систем.

Доктрина 2000 определяла под информационной безопасностью Российской Федерации состояние защищенности национальных интересов в информационной сфере.

В Доктрине 2000 были закреплены четыре основные составляющие национальных интересов Российской Федерации в информационной сфере:

- соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;
- информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам;
- развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности;
- защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

До настоящего времени в полном объеме не реализован комплекс мер по развитию нормативно-правовой базы в сфере информационной безопасности, определенный поставленным кругом задач:

- разработка основных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации, а также мероприятий и механизмов, связанных с реализацией этой политики;
- развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Российской Федерации, а также системы противодействия этим угрозам;
- разработка федеральных целевых программ обеспечения информационной безопасности Российской Федерации;
- разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации, а также сертификации этих систем и средств;
- совершенствование нормативной правовой базы обеспечения информационной безопасности Российской Федерации, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации;
- установление ответственности должностных лиц федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности;
- координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, предприятий, учреждений и организаций независимо от формы собственности в области обеспечения информационной безопасности Российской Федерации;
- развитие научно-практических основ обеспечения информационной безопасности Российской Федерации с учетом современной геополитической ситуации, условий политического и социально-экономического развития России и реальности угроз применения "информационного оружия";
- разработка и создание механизмов формирования и реализации государственной информационной политики России;

- разработка методов повышения эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;
- обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность, и в первую очередь в области создания специализированной вычислительной техники для образцов вооружения и военной техники;
- разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;
- развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;
- создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;
- расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;
- обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;
- создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

По поводу Доктрины 2000 имеется мнение Е.К. Волчинской о том, что: «Понятие информационной безопасности в соответствии с Доктриной информационной безопасности Российской Федерации носит достаточно общий характер, оно включает как защиту информации, так и, образно говоря, защиту от информации, а также защиту информационных сетей и систем, защиту прав и свобод, связанных с информацией (в том числе прав на доступ к информации, интеллектуальных прав, свободы массовой

информации). Такое многообразие задач затрудняет координацию усилий различных органов власти, полномочия которых так или иначе распространяются на регулирование информационной сферы»[62]. При этом следует иметь в виду, что на момент написания данной статьи Волчинскя Е.К. занимала должность ведущего советника аппарата Комитета Государственной Думы по безопасности, т.е. в статье, в значительной мере, нашла свое отражение «официальная» точка зрения.

В настоящее время в Российской Федерации Доктрина информационной безопасности утверждена Указом Президента Российской Федерации от 5 декабря 2016 года № 646 «Об утверждении доктрины информационной безопасности Российской Федерации» (далее: «Доктрины»), что снимает имевшийся неопределенный правовой статус системы официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. При этом специально указано, что Доктрина является документом стратегического планирования в сфере обеспечения информационной безопасности российской Федерации, в котором развиваются положения Стратегии национальной безопасности Российской Федерации[63], а также других документов стратегического планирования в указанной сфере.

При этом под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в сети интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Под информационной безопасностью Российской Федерации в новой Доктрине понимается состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечивается реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально- экономическое

[62] Волчинская Е.К. Информационное право, 2008, № 4
[63] Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // http://www.pravo.gov.ru, 31.12.2015

развитие Российской Федерации, оборона и безопасность государства. Обеспечение информационной безопасности представляет собой осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидация последствий их выявления.

В качестве национальных интересов в информационной сфере определены:

- обеспечение и защита конституционных прав и свобод граждан Российской Федерации в информационной сфере;

- обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры;

- развитие в России отрасли информационных технологий и электронной промышленности;

- доведение до общественности достоверной информации о государственной политике Российской Федерации;

- содействие формированию системы международной информационной безопасности.

В Доктрине осуществлен анализ угроз в сфере информационной безопасности, к которым отнесены:

- использование трансграничного оборота информации для достижения геополитических, террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности;

- наращивание возможностей информационно-технического воздействия в военных целях при одновременном усилении технической разведки в отношении России;

- использование специальными службами иностранных государств средств оказания информационно-психологического воздействия, увеличение объема информации, содержащей негативную оценку государственной политики Российской Федерации;

- осуществление информационного воздействия различными террористическими и экстремистскими организациями на индивидуальное,

групповое и общественное сознание, а также на критической информационной инфраструктуры;

- рост компьютерной преступности.

Доктрина определяет стратегические цели и основные направления информационной безопасности, которым относятся:

- в области обороны страны, - защита жизненно важных интересов от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, в т.ч. в целях осуществления враждебной деятельности и актов агрессии;

- в области государственной и общественной безопасности , - защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности, обеспечение основных прав и свобод, защита критической информационной инфраструктуры;

- в экономической сфере, - сведение к минимуму влияние негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли информационных технологий и электронной промышленности, разработка и производство средств обеспечения информационной безопасности, повышение объемов и качества оказания услуг в сфере информационной безопасности;

- в области науки, технологий и образования, - поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности;

- в области стратегической стабильности и равноправного стратегического партнерства путем создания системы неконфликтных межгосударственных отношений в информационном пространстве.

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере. Состав системы

обеспечения информационной безопасности определяется Президентом Российской Федерации. Организационную основу составляют: Совет Федерации ФС РФ, Государственная Дума ФС РФ, правительство Российской Федерации, федеральные органы исполнительной власти, Центральный Банк РФ, Военно-промышленная комиссия РФ, межведомственные органы, органы местного самоуправления, органы судебной власти, - принимающие участие в решении задач по обеспечению информационной безопасности в соответствии с требованиями законодательства.

Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане.

Доктриной также определена совокупность принципов и задач государственных органов в рамках деятельности по обеспечению информационной безопасности.

Обращает на себя внимание то обстоятельство, что в нормах федерального законодательства термин «безопасность информации» практически не используется. Отраслевое законодательство информационного права оперирует понятием понятие защиты информации, которая ст. 16 Закона «Об информации» определяется как принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

- соблюдение конфиденциальности информации ограниченного доступа;

- реализацию права на доступ к информации.

Следует полагать, что защита информации представляет собой деятельность, идеальным результатом которой является безопасность информации как состояние, максимально согласующееся с четырьмя основными составляющими национальных интересов Российской Федерации в информационной сфере.

По мнению А.А. Стрельцова ряд норм, образующих нормативное правовое обеспечение информационной безопасности, развивают правовые механизмы, регулирующие общественные отношения, относящиеся к другим отраслям права, в том числе таким базовым отраслям, как конституционное, гражданское, административное и уголовное право[64]. При этом правовое обеспечение информационной безопасности базируется на совокупности институтов и норм информационного, конституционного, гражданского, административного и уголовного права, регулирующих отношения в области противодействия угрозам безопасности объектов национальных интересов в информационной сфере.

[64] Стрельцов А.А. Теоретические и методологические основы правового обеспечения информационной безопасности России: дисс.... д.ю.н. М., 2004. С. 146.

Глава 2. Правовые методы обеспечения информационной безопасности

2.1. Характеристика информации, как объекта обеспечения безопасности в Российской Федерации

Внутренним правовым противоречием информационного общества представляется проблема использования информационных ресурсов, при которой, с одной стороны, право на информацию является обязательным компонентом общественной жизни, с другой стороны, наличие или отсутствие информации является основой успешности политической, общественной, либо хозяйственной деятельности.

При этом можно выделить ряд значимых подходов к информации[65]:

- теоретико-отражательный, раскрывающий информацию как определенную характеристику отображения объективной действительности, которой сопровождаются все протекающие в мире процессы[66], когда информация используется для описания и объяснения отражаемых явлений;

- гносеологический (когнитивный), представляющий информацию как средство познания, т.е. информация рассматривается как сообщения о фактах, событиях, процессах, явлениях и т.п.;

- семантический, предполагающий содержание и практическую ценность информации;

- аксиологический, формирующий концепции ценности информации для различных сфер деятельности;

- количественный, приобретающий значение для принятия решения;

- коммуникативный, раскрывающий сложную организационно-техническую природу информационных связей, когда информация воспринимается как совокупность сигналов, воздействий или сведений, которые некоторая система воспринимает от окружающей среды (входная

[65] Боруленков Ю.П. Об информационно-интерпретационной сущности юридического познания. Часть 1. Информация как явление отражения взаимодействия объектов // Российский следователь. 2013. № 7. С. 6 - 12.

[66] Урсул А.Д. Отражение и информация. М., 1973. С. 114; Соколов А.В. Информационный подход в системе документальных коммуникаций. Л., 1987. С. 18 - 19.

информация), выдает в окружающую среду (выходная информация) или хранит в себе (внутренняя, внутрисистемная информация)[67];

- нормативно-правовой, раскрывающий содержание правовых явлений. Раскрывая правовой статус информации, в первую очередь обращает на себя внимание дефиниция, определенная Законом «Об информации, информационных технологиях и о защите информации»[68] (Законом Об информации), согласно которому информация определяется как сведения (сообщения, данные), вне зависимости от формы их представления. В легальном определении находит свое отражение необходимость взаимосвязи информации как явления материального мира с проблемами его познания, т.е. определения, передачи, сохранения свойств, параметров и характеристик предметов, явлений и процессов, когда на первый план выходит понятие информации, ее характеристики и свойства. Собственно, указанная точка зрения сопрягается с научным восприятием информации как результата отражения, когда осуществляется «процесс и результат воздействия одной материальной системы на другую, который представляет собой воспроизведение в иной форме особенностей (черт, сторон, структуры) одной системы в особенностях (чертах, структуре) другой системы»[69]. Отражение при этом соотносится с философскими категориями материи, движения, пространства, времени, энергии и поля.

Формирование подхода к информации как к результату отражения следует связывать с необходимостью получения результатов от практического использования знаний об информации.

Впервые о теории информации упомянуто в конце 40-х годов прошлого века в работе К.Шеннона[70], однако уже к середине 50-х годов ученые стали различать количество и качество информации[71]. Следующим закономерным шагом стало различие подходов к информации как феноменальной

---

[67] Дородницын А.А. Информатика: предмет и задачи // Кибернетика. Становление информатики. М., 1986. С. 22.
[68] СЗ РФ, 31.07.2006, № 31 (1 ч.), ст. 3448
[69] Посков Я.А. Основы информационного обеспечения производства следственных и процессуальных действий / Под ред. В.А. Шурухнова. М., 2010. С. 6.
[70] Shannon C.E. Mathematical Theory of Communication // Bell System Technical Journal. 1948/ Vol. 27. P. 379 - 423
[71] MacKayD., Information, mechanism and meaning. Cambridge and London. 1969

характеристике свойств материи: стали выделять математический, семантический и прагматический подходы[72].

В семидесятые годы того же века А.С. Пресман выделяет основные качественные параметры информации:

- организационную роль информации в физических системах;

-передачу и прием системами информации об их организации;

- неявность информации в неживых системах;

- слабость информационных воздействий по сравнению с вещественно-энергетическими эффектами для живых систем;

- необходимость и возможность рассмотрения любой биосистемы в качестве кибернетической, вне зависимости от ее структурной организации.

При этом Пресман А.С. полагал под информацией только результат отражения одного объекта в другом, используемый для формирования управляющих воздействий[73].

Шрейдером Ю.А. разработана семантическая теория информации, во главу угла ставящая свойства приемника (получателя) информации, воспринимающего и накапливающего информацию, оценивая ее смысловое (семантическое) значение[74].

Обращает на себя внимание то обстоятельство, что в середине прошлого века вопросу о материальной сущность информации посвящалось значительное количество работ ученых различных отраслей знания, включая ученых-философов[75].

При этом исходили из того, что по мере развития естествознания, к двум основным формам реальности (веществу и энергии) добавлено понятие «поле». Далее, Н. Винер предложил рассматривать основу всего существующего как единство вещества и поля, с одной стороны, информации — с другой, и энергии — с третьей.

Ссылаясь на высказывание Н.Винера о том, что информация есть информация, а не материя и не энергия, следует иметь в виду, что далее он

---

[72] Городов О.А. Информационное право. Учебник. М., С. 32

[73] Пресман А.С. Организация биосферы и ее космические связи. М., 1997.С.93

[74] Шрейдер Ю.А. Социальные аспекты информатики // НТИ. 1989. С. 3-14.

[75] Павлов Т. Информация, отражение, творчество. М., 1967; Украинцев Б. С. Отражение в неживой природе. М., 1969; Тюхтин В. С. Отражение, системы, кибернетика. М., 1972; Бирюков Б. В. Кибернетика и методология науки. М., 1974; Урсул А. Д. Отражение и информация. М., 1973; Цонев В. Информация и отражение. София, 1977; Янков М. Материя и информация. София, 1976; Гришкин И. И. Понятие информации. М., 1973

указал: «Тот материализм, который не признает этого, не может быть жизнеспособен в настоящее время»[76]. Таким образом, в основе информационных отношений лежит материальная сущность информации.

В современной науке содержание материи понимается как единство вещества, поля и плазмы, порождаемых флуктуациями вакуума. Кроме того, в понятие материи включается информационный аспект существования всех материальных систем, который выражает порядок вещей и явлений в материальном мире[77].

По мнению В.Н.Лопатина, в науке возникают два противоречащих подхода к информации – атрибутивный и функциональный[78]. Атрибутивный трактует информацию как свойство всех материальных объектов, атрибут материи, делая акцент на независимость информации от процесса ее использования (статический аспект информации); функциональный подход связывает информацию лишь с функционированием самоорганизующихся систем, определяя ее через динамику информационных процессов (динамический аспект информации).

При этом выделяются внутренняя и внешняя информация, причем внутренняя (структурная, связанная) информация рассматривается как характеристика организованности любой системы и возникает как результат отбора, фиксации и закрепления в системе в форме определенных структурных изменений ее положительного опыта взаимодействия с внешней средой. Внешняя (относительная, оперативная, рабочая) информация определяется как средство организации любой системы и раскрывается через связь с отражением.

Связывая информацию с отражением выделяют прямое и косвенное типы отражений. Прямое отражение представляет собой все формы контактного отражения, - изменения положения, структуры, формы, контура, величины и других параметров отражающего объекта под его воздействием с отражаемым объектом. Косвенное отражение имеет место в тех случаях, когда отсутствует непосредственный контакт между

[76] Винер Н. Кибернетика или управление и связь в животном и машине. М., 1958
[77] Основы современной философии. СПб.:1999. С. 57
[78] Лопатин В.Н. Информационная безопасность России. дис. д.ю.н., Санкт-Петербург. 2000. С 27; Веселовский В.Н. О сущности живой материи. М., 1971.

отражаемым и отражающим объектами, отражение опосредуется через передающую среду отражения.

По аналогии с видами доказательств[79] можно выделять материально–фиксированную (вещную, вещественную) и психофизиологическую (личностную, личную) формы отражения, при этом к вещной форме следует относить объективную фиксацию признаков в материальном мире (отождествление), к психофизиологической – субъективное отображение мысленного образа в сознании человека (узнавание)[80].

По мнению Ф.Энгельса «тождество с собою имеет своим необходимым дополнением отличие от всего другого»[81]. В основу узнавания или отождествления могут быть положены философские категории о тождественности объектов и явлений материального мира, их обусловленности, взаимосвязи и взаимозависимости. Материалистическая теория отражения как свойства живой и неживой материи рассматривает закономерности отображения как результата действий, закономерности суждения по отображению о свойствах отобразившегося объекта или явления, закономерности использования полученных данных для составления целостной картины описываемого процесса или явления. Получение информации и ее запоминание являются той основой, на которой строятся все практические действия[82]. «Память представляет собой сложный психический процесс, включающий в себя: запоминание предметов, явлений, лиц, действий, мыслей, информации и т. д.; сохранение в памяти того, что было запомнено; узнавание при повторном восприятии и воспроизведение запомненного».

Таким образом, деятельность по представлению информации об объекте, предмете или явлении представляет собой физическую деятельность по изысканию, фиксации и анализу изменений в окружающем мире, произошедших в результате взаимодействия материальных объектов, основывающуюся на следующих принципах:

---

[79] Вандышев В. В. Уголовный процесс. Курс лекций. СПб, 2002. С.45; Уголовный процесс: Учебник для вузов / Л.К. Айвар, Н.Н. Ахтырская, Э.И. Бордиловский и др.; под ред. В.И. Радченко. 2-е изд., перераб. и доп. М.:, 2006. С. 82

[80] Елин В.М., Жарова А.К. К вопросу о методологии информационного права. Право и государство: теория и практика. 2013. № 4 (100). С 133-143.

[81] Энгельс Ф. Диалектика природы. Маркс К., Энгельс Ф. Соч. Т. 20. С. 530

[82] Чуфаровский Ю.В. там же С. 39

- любое явление материального мира может быть индивидуально определено и должно обладать устойчивым строением;

- совокупность представляемых отражений свойств явления материального мира включает в себя также и взаимосвязь между отражаемым объектом и окружающей средой;

- информация об объекте, предмете или явлении представляет собой практическую деятельность по отображению устойчивых свойств объектов;

- информация об объекте, предмете или явлении возникает в результате взаимодействия с окружающей средой и характеризует совокупность изменений, внесенных в окружающую среду.

Разрешая вопрос о достаточности информации, следует ограничивать объем информации, связывая ее лишь с теми измененными характеристиками окружающего мира, которые дают наиболее четкое представление об интересующих нас объектах, процессах и явлениях.

Использование при этом математического аппарата при современном уровне развития науки представляется возможным, но излишне громоздким, излишне усложняющим построение моделей в повседневной деятельности, однако оправданным для решения отдельных информационных задач. «Существующая возможность построения математических моделей идентификации объектов, процессов или явлений сталкивается с проблемой ……избыточности информации, когда … проблема качества информации, поиски меры, где могут соединяться количественные и качественные определения, по сути, связана с вопросами о собственной ее структурности, а в силу коррелятивности понятий структуры и системы – также с понятием системности информации»[83].

По всей видимости, именно поэтому, все науки, осуществляющие активное использование информации, деликатно обходят стороной вопрос о материальности информации как таковой, категорически настаивая на материальности информации в свЯзи с ее носителем.

Итак, информация существует объективно, но воспринимается всегда субъективно. При этом возникает взаимосвязь между информацией и ее материальным носителем. При взаимодействии информации и носителя свойства каждого из них в значительной мере изменяются.

[83] Кремлянский В.И. Методологические проблемы системного подхода к информации. М.. 1977

Фиксация полученных результатов может осуществляться путем документирования информации, причем наиболее разработаны методики документирования с надлежащими реквизитами лишь на бумажном носителе. При этом как реквизиты, так и содержание документа фиксирует не только фактическую информацию об интересующих нас изменениях в окружающем мире, но также процесс ее получения и фиксации.

Вполне закономерным представляется необходимость выделения характеристик информации именно в ее связи с носителем, что приводит нас к пониманию сущности информационного объекта и, далее, к понятию документированной информации.

При этом следует обращать внимание на особенности и свойства информации, приобретающие существенное значение[84]:

«- свойство физической неотчуждаемости основано на том обстоятельстве, что знания не отчуждаемы от человека, их носителя, в связи с чем при передаче информации от одного лица к другому процедура отчуждения информации должна заменяться передачей прав на ее использование;

- свойство обособляемости информации основано на том, что включаемая в оборот информация всегда овеществляется в виде символов, знаков, волн, вследствие этого обособляется от ее производителя (создателя) и существует отдельно и независимо от него;

- свойство информационной вещи (информационного объекта) возникает в силу того, что информация передается и распространяется только на материальном носителе или с помощью материального носителя, и проявляется как «двуединство» информации (ее содержания) и носителя, на котором эта информация (содержание) закреплено, вследствие этого на носитель распространяется институт вещного права, а на информацию – институт информационного права». При этом следует иметь в виду, что в нормативных актах закреплено понятие документированной информации, под которой понимается зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель[85];

---

[84] Копылов В.А. Информационное право: Учебник. — М., 2002. — С. 24

[85] П. 11 ст.2 ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации№

«- свойство тиражируемости (распространяемости) информации основано на том, что информация может тиражироваться и распространяться в неограниченном количестве экземпляров без изменения ее содержания (одна и та же информация (содержание) может принадлежать одновременно неограниченному кругу лиц (неограниченный круг лиц может знать содержание этой информации);

- свойство организационной формы связано с тем, что информация, находящаяся в обороте, как правило, представляется в документированном виде;

- свойство экземплярности информации заключается в том, что информация распространяется, как правило, не сама по себе, а на материальном носителе, вследствие чего возможен учет экземпляров информации через учет носителей, содержащих информацию.»

Таким образом, практическое правовое регулирование информационных процессов осуществляется в пределах предоставленных прав при использовании документированной информации.

Право на информацию неразрывно связано с развитием гражданского общества, первоначально находя свое отражение в Декларации прав человека и гражданина периода Великой французской революции, Конституции США, Конституции Швеции, документах Лиги Наций. Конституция СССР 1936 года предоставляла гражданам ряд информационных прав, включая[86] свободу слов и, печати, неприкосновенность тайны переписки граждан.

Однако подлинный всплеск развитие информационных прав и свобод получило после второй мировой войны с принятием Организацией объединенных наций Всеобщей декларации прав человека 1948 года, в ст. 19 определившей «свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ»[87]. Дальнейшее закрепление данный принцип получил в ст. 19 Международного пакта о гражданских и политических правах[88], оправляющей, с одной стороны «право на свободное выражение своего мнения; это право включает свободу

[86] Конституция (Основной Закон) Союза Советских Социалистических Республик (утв. Постановлением Чрезвычайного VIII Съезда Советов СССР от 05.12.1936)

[87] Всеобщая декларация прав человека (Принята 10.12.1948 Генеральной Ассамблеей ООН)

[88] Ведомости ВС СССР. 28 апреля 1976 г. № 17. Ст. 291.

искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения или иными способами по своему выбору», а с другой стороны, появление специфических обязанностей и ответственности, возникающих как результат пользования информационными правами и свободами. Ограничение права на информацию должно устанавливаться только законом и быть направленным на охрану государственной безопасности, общественного порядка, здоровья или нравственности населения.

Данный подход стал основой в формировании как государственных, так и межгосударственных принципов построения информационного общества, найдя свое отражение, например в Конвенции Совета Европы о защите прав человека и основных свобод (1950 года), конституциях стран Европейского союза, Конституции Российской Федерации.

Вообще, по мнению В.Н.Лопатина, в Конституции Российской Федерации 1993 года, примерно третья часть гражданских прав и свобод так или иначе связана с информационными правами. Статья 24 Конституции РФ напрямую закрепляет право граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Существующие ограничения принципа определяются федеральным законодательством.

Дальнейшее развитие указанный конституционный принцип получил в Законе «Об информации, информатизации и защите информации» (1995 года)[89] и в пришедшем ему на смену ФЗ № 149 «Об информации, информационных технологиях и о защите информации»[90] (2006 года) (Далее – Закон «Об информации»).

Статья 5 Закона об информации подразделяет информацию по категориям доступа к ней на общедоступную и информацию ограниченного доступа. В основе такого деления лежит существование ограничений доступа к информации федеральными законами. В зависимости от порядка ее предоставления или распространения информация подразделяется на

[89] Федеральный закон от 20.02.1995 № 24-ФЗ "Об информации, информатизации и защите информации"// СЗ РФ 20.02.1995, № 8, ст. 609,Утратил силу в связи с принятием Федерального закона от 27.07.2006 № 149-ФЗ

[90] СЗ РФ, 31.07.2006, № 31 (1 ч.), ст. 3448,

свободно распространяемую; предоставляемую по соглашению лиц, участвующих в соответствующих отношениях; подлежащую предоставлению или распространению; а также информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Таким образом, с точки зрения отраслевого законодательства единственным критерием ограничения доступа к информации является наличие прямого запрета в федеральном законодательстве, ограничивающего информационные права и свободы граждан.

По мнению И.Ю.Богдановской «Российский законодатель, устанавливая требования к информации, не отнесенной к информации ограниченного доступа, а также требования к условиям доступа и ее распространения, использует следующие понятия:

- открытая информация;
- общедоступная информация;
- открытая и общедоступная информация;
- информация, являющаяся общественным достоянием;
- информация особой социальной значимости (социально значимая информация)».

Раскрывая понятия, авторы определяют под общедоступной информацией сведения, открытые для ознакомления, познания. Общедоступная информация не становится объектом гражданского права, может свободно и безвозмездно использоваться и распространяться любым лицом.

Понятие открытой информации авторами в целом не раскрывается, однако уточняется, что в ряде случаев режим открытой информации не отличается от режима общедоступной информации, в некоторых случаях правовой режим определяется рядом элементов, к которым относятся: круг лиц; форма предоставления информации (в виде выписок); доступ к информации, объем предоставляемой информации, платность предоставления информации и т.д.

Открытая и общедоступная информация характеризуется следующим режимом: неограниченностью круга лиц, имеющих право получать информацию, различные формы предоставления информации; как правило, неустановленная цель предоставления информации, безусловно открытый

доступ, неограниченный объем предоставления информации, гарантии соблюдения режима.

Информация как общественное достояние терминологически достаточно широко используется, в первую очередь, в международных документах по формированию информационного общества: «Информацией, являющейся общественным достоянием, считается доступная для населения информация, использование которой не нарушает никаких предусмотренных законом прав или обязательств по соблюдению конфиденциальности»

Информация, представляющая особую социальную значимость, является открытой информацией, которая имеет значение для всего общества в целом и сокрытие которой может отрицательно сказаться на реализации прав и свобод человека[91].

По мнению В.А. Дозорцева, информация, "содержащаяся в опубликованных источниках, как не была так и не стала объектом гражданского права, она коммерческой ценности не представляет"[92]. Следовательно, ценность для экономического оборота представляет только необщедоступная информация, в связи с чем только она может быть объектом правовых отношений. А.А. Самохвалов считает, что к общедоступной информации может быть отнесена информация, которая должна быть раскрываема без ограничений, то есть на которую нельзя установить свое господство в связи с законодательным ограничением, либо такая информация является общеизвестной, распространяемой, например, средствами массовой информации[93].

По мнению Г. Отнюковой открытую информацию следует подразделять на общедоступную и незакрытую. При этом под незакрытой информацией понимается информация, не относящаяся ни к категории общедоступной, ни к информации ограниченного доступа[94].

---

[91] Право на доступ к информации. Доступ к открытой информации/ Отв. Ред.И.Ю.Богдановская._М., 2009, С. 32-48.

[92] Дозорцев В.А. Интеллектуальные права: Понятие. Система. Задачи кодификации. Сборник статей. М., 2005. С. 228.

[93] Самохвалов А.А. Информация как объект гражданских прав // http://www.yurclub.ru/docs/pravo/1503/4.html.

[94] Отнюкова Г. Коммерческая тайна// Закон.- 1998. № 2. С. 55.

Высказывалась также точка зрения о необходимости выделения самостоятельной категории информации, сведения и данные, относящиеся к которой, доступны только лицам, обладающим специальным статусом[95].

По мнению З.З. Зейналова[96], следует выделять категорию неизвестной информации, которую можно разделить на две подгруппы - условно доступную и недоступную. К категории условно доступной следует относить научные гипотезы, аргументированные предположения, абстракции, недоказанные утверждения, догадки и т.д. К недоступной информации предлагается отнести информацию о тех явлениях, которые существуют, но научно их доказать невозможно или же ненаучно предполагается вероятность их существования. Отличием условно доступной информации от недоступной информации является научная обоснованность.

При этом то обстоятельство, что в классификациях рассмотрены частные случаи общедоступной информации, следует считать недостатком предлагаемых классификаций.

Например, в 2013 году выделена категория общедоступной информации, определяемая как открытые данные, т.е. информация, содержащаяся в информационных системах и ресурсах, предоставляемая юридическими лицами, которая подлежит размещению в информационно-телекоммуникационной сети общего пользования Интернет в соответствии с законодательством Российской Федерации, и может свободно использоваться любыми лицами[97].

Следует также иметь в виду, что результаты интеллектуальной деятельности в общем случае относятся к информации, размещаемой в форме открытых данных. Однако существуют предусмотренные законом жесткие ограничения на использование произведений в любой форме и любым не противоречащим закону способом. Согласно требованиям ст. 1229 ГК РФ правообладатель может по своему усмотрению разрешать или запрещать другим лицам использование результата интеллектуальной

[95] Богданов В.М. Информация как объект гражданских прав. Дис. канд.юрид.наук.- Екатеринбург. 2005.
[96] Зейналов З.З. Проблемы определения информации как объекта информационных правоотношений // Информационное право. 2010. № 1. С. 6 - 9.

[97] Указ Президента РФ от 07.05.2012 № 601 «Об основных направлениях совершенствования системы государственного управления» // СЗ РФ, 07.05.2012, № 19, ст. 2338; Постановление Правительства Москвы от 02.04.2013 № 187-ПП «Об автоматизированной информационной системе «Общегородская платформа открытых данных» // Официальный сайт Правительства Москвы http://www.mos.ru, 10.04.2013

деятельности или средства индивидуализации. В результате заключения лицензионного договора лицензиар предоставляет или обязуется предоставить другой стороне право использования такого результата или такого средства в предусмотренных договором пределах. Нарушение установленных требований порождает гражданско-правовые, административные и уголовные последствия. Таким образом, возникает необходимость в введении дополнительных классов общедоступной информации. Однако, в ряде случаев, предусмотренных ст.ст. 1272 - 1280 ГК РФ, существует возможность ограниченного использования некоторых результатов интеллектуальной деятельности без согласия правообладателя и без выплаты ему вознаграждения. Таким образом, в зависимости от существующих информационных процессов, информация может быть отнесена, а может быть и не отнесена к вводимой дополнительной категории. Существующим законодательством определена инсайдерская информация98 как точная и конкретная информация, которая не была распространена или предоставлена (тайна как частный случай) распространение или предоставление которой может оказать существенное влияние на цены финансовых инструментов, иностранной валюты и (или) товаров и которая относится к информации, включенной в соответствующий перечень инсайдерской информации, утвержденными Приказом Федеральной службы по финансовым рынкам, Банком России, органами управления государственных внебюджетных фондов, органами исполнительной власти и т.д. При этом обращает на себя внимание то обстоятельство, что инсайдерская информация может являться информацией ограниченного доступа только в частном случае, когда относится к банковской, налоговой тайне, тайне связи и т.д. Фактически данным законом, в обход требований международного права и конституционных принципов вводится дополнительная категория информации не по доступу к ней, а по процедуре отнесения.

Таким образом, классификатор общедоступной информации следует дополнить рядом категорий информации, куда следует отнести результаты интеллектуальной деятельности, инсайдерскую информацию, возможно

[98] Федеральный закон от 27.07.2010 № 224-ФЗ "О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации" // СЗ РФ, 02.08.2010, № 31, ст. 4193.

информацию, размещаемую в СМИ, публичную оферту и т.д. Однако введение дополнительных классов представляется не совсем оправданным, по следующей причине:

В конце 2008 – начале 2009 годов в Российской Федерации приняты Федеральные законы от 22.12.2008 N 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»[99] и «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 09.02.2009 N 8-ФЗ[100]. При определении способов обеспечения доступа к информации о деятельности, законом предусматривается в т.ч. и превентивное обнародование (опубликование) информации о деятельности в СМИ, а также размещение информации о деятельности в сети "Интернет". При этом сохраняется возможность предоставления пользователям информации о деятельности по их запросу.

Таким образом, с принятием указанных законов содержание права на доступ к информации, ранее включавшее в себя возможность поиска и получения любой информации в любых формах и из любых источников (что предполагает активную деятельность лиц, желающих обладать информацией), расширилось за счет обнародования, размещения и ознакомления (что возлагает на обладателя информации ряд обязанностей информационного характера и допускает определенную пассивность в действиях лиц, заинтересованных в получении информации).

Таким образом, появляется возможность классификации общедоступной информации по осуществляемым в отношении нее информационным процессам, включающим в себя возможность свободного поиска, получения, передачи, производства и распространения общедоступной информации любым законным способом. При этом особое значение приобретает вопрос об объеме информации, ее достаточности, о количестве и качестве получаемой общедоступной информации.

Существующие информационные права и гарантии ограничиваются в соответствии с требованиями ч. 3 ст. 55 Конституции РФ, согласно требованиям которой права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо

[99] СЗ РФ № 52 (ч. 1), ст. 6217, 29.12.2008
[100] СЗ РФ 16.02.2009, № 7, ст. 776

в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства[101].

Конституционным судом РФ определено, что уровни гарантий и степень возможных ограничений права на получение информации в соответствии с «федеральным законом, устанавливающим специальный правовой режим не подлежащей распространению информации, обусловленный ее содержанием, в т.ч. наличием в ней данных, составляющих государственную тайну, конфиденциальных сведений, связанных с частной жизнью, со служебной, коммерческой профессиональной, изобретательской деятельностью»[102].

Согласно ст. 9 Закона «Об информации» обязательным условием отнесения информации к информации ограниченного доступа является наличие ограничения доступа к информации данной категории в федеральных законах. Целью ограничения доступа к информации является защита основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. При этом в отношении информации ограниченного доступа обязательным является соблюдение конфиденциальности информации.

Информация ограниченного доступа в первую очередь ассоциируется федеральным законодателем с понятием «тайна»[103], причем в федеральных законах нашей страны встречается, по разным подсчетам от 40 до 100 видов тайн.

В дореволюционной юридической литературе «тайна» определялась в основном, как «сохранение в негласности обстоятельства, разглашение которого принесло бы больше вреда, чем пользы, понимая последнюю не только в смысле утилитарном, но и в смысле отвлеченном, т.е. ограждение существования и питания нравственных идеалов человеческого

[101] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // СЗ РФ, 26.01.2009, № 4, ст. 445

[102] Определение конституционного суда Российской Федерации от 23 июня 2005 года № 300 – О

[103] См., например: *Кузьмин С.В.* Тайна в уголовном праве. Автореф. дисс... канд. юрид. наук. - Ставрополь: Ставропольский государственный университет, 2000; Суслова С.И. Тайна в праве России: цивилистический аспект. дисс. канд.юр. наук; Михайлов В.М. Право па тайну. // Закон. - 1998. - № 2; Гайнуллина З.Ф. Правовое обеспечение прав и законных интересов обладателей необщедоступной информации (коммерческой тайны, ноу-хау): Дисс. канд. юр. наук.-М., 1998; Смолькова И.В. Проблемы охраняемой законом тайны в уголовном процессе. -М.: Луч, 1999

совершенствования». С сожалением приходится констатировать, что в настоящее время, в словарях и справочных изданиях понятие «тайна» практически не упоминается. Большая Советская Энциклопедия включает информацию только о двух видах тайны - государственной и переписки[104].Как «нечто скрываемое от других, известное не всем, секрет» определяет тайну СИ. Ожегов в Словаре русского языка[105]. В толковом словаре В. Даля[106] тайна представлена в двух значениях: в широком смысле: «тайна - кто чего не знает, то для него тайна; все сокрытое, неизвестное, неведомое»; и в узком смысле: «тайна - нечто скрытно хранимое, что скрывают от кого-либо с намерением таять».

Кузьмин С.В., рассматривая «тайну» с точки зрения филологического подхода, делает интересный вывод о том, что, данный термин в русском языке имеет два смысловых значения: «нечто абсолютно неизвестное всем и нечто относительно неизвестное для какого-либо круга лиц. Очевидно, что правовое значение имеет только второе значение исследуемого термина»[107]. Далее автор делает вывод о том, что чрезвычайно важным аспектом в исследовании тайны является ценность информации, которая может иметь незначительную (обычную) ценность, значительную ситуативную (условную) ценность (при информационном дефиците), значительную содержательную ценность. При этом определено, что только та информация, которая имеет значительную ценность и затрагивает наиболее важные сферы общественной жизни может стать содержанием охраняемой законом тайны.

Рядом исследователей определяется, что тайну следует рассматривать[108] как единство ее субъективного и объективного аспектов. Очевидно, что содержанием тайны является информация особого рода, обладающая рядом специфических признаков, обуславливающих объективную необходимость (возможность) распространения на нее правового режима ограничения доступа. Тайна будет наделена правовой защитой только тогда, когда ее режим предусмотрен законом, причем, в зависимости от специфики того или иного вида тайны, проявление воли обладателя информации не всегда

---

[104] *Большая* Советская Энциклопедия. / Гл. ред. *А.М. Прохоров.* - В 30 т.-Изд-с3-е-М.: Сов. Энциклопедия, 1976. Т. 25.-С, 214.

[105] *Ожегов СИ.* Толковый словарь русского языка. / СИ. Ожегов, Н.Ю. Шведова. -4-ое изд., дополненное. - М., 1999 - С. 250.

[106] *Даль В.* Толковый словарь. -М., 1955.-Т. 4.-с. 386.

[107] *Кузьмин С.В.* Указ. соч. -С. 8.

[108] Суслова С.И. Указ. соч.

является обязательным, хотя в некоторых случаях должна быть необходимым условием ограничения доступа к сведениям.

Мнения зарубежных, советских и российских исследователей по поводу сущности тайны можно разделить на две группы:

Сущность позиции первой группы основана на - противопоставлении тайны и принципа гласности по содержанию. При этом тайна оценивается как «исключение из принципа гласности». Так, И. Бентам считал, что[109] «тайна в судопроизводстве составляет зло», мотивируя это тем, что «принцип исключения вреден или по своему направлению, или по своему действию,... потому что увеличивает вероятность успеха для всех несправедливых дел». При этом тайна рассматривается как информационный феномен, исключаемый из публичности, входящий в противоречие с принципом гласности, когда тайна, ограничивая действие принципа гласности, представляет самостоятельный правовой институт;

Вторая группа - характеризует тайны как один из видов информации, либо в качестве «документированной информации, имеющей какую-либо ценность[110]», либо в качестве конфиденциальной информации.

В целом, суммируя высказываемые по поводу тайны точки можно выделить ряд методологических положений, связанных с правовым феноменом тайны:

- под тайной, являющейся объектом правового регулирования следует понимать специфическую информацию, скрываемую субъектом от других членов общества, в силу необходимости решения специфических задач обеспечения информационной безопасности личности, общества и государства;

- обязательным условием отнесения информации к тайне является требование федерального закона об отнесении информации данной категории к информации ограниченного доступа, в связи с чем необходимо отличать тайну в правовом смысле и иную скрываемую в обществе информацию;

- тайна характеризуется единством составляющей информации и правового режима ограничения доступа к ней;

---

[109] *Бентам И.* О судоустройстве. - Спб,, 1860. -201 с.

[110] См.: *Демушкин А,С.* Документы и тайна. - М.: ООО «Городец-издат», 2003.-354 с.

- в отношении информации, относящейся к тайне, применяются специальные правовые режимы, основным назначением которых является решение задачи защиты информации ограниченного доступа;

- законодательное требование отнесения информации к тайне является единственным правовым основанием ограничения доступа к информации;

- реализация защиты информации в отношении информации ограниченного доступа состоит в соблюдении конфиденциальности такой информации, в то время как для общедоступной информации, - в реализации права на доступ к информации.

Ограничение доступа к информации, не подпадающей под категорию тайн, является незаконным, поскольку противоречит требованиям Конституции Российской Федерации, российского и международного законодательства.

Наряду с категорией «тайн» в нормативно-правовых актах и юридической литературе встречается понятие «конфиденциальности (конфиденциальной) информации». По результатам выборки статьи с таким наименованием встречаются в 100 федеральных законах, а всего данное словосочетание используется более чем в 3000 нормативных актов.

При этом зачастую использование данного понятия идет вразрез с требованиями законодательства. Так, ФНС РФ в локальном нормативном акте раскрывает данное понятие следующим образом: «...Конфиденциальная информация - требующая защиты информация, доступ к которой ограничивается в соответствии с действующим законодательством Российской Федерации, а также настоящим Регламентом...»[111].

Между тем, ст. 2 Закона «Об информации» дает определение «конфиденциальности информации» как обязательного для выполнения лицом, получившим доступ к определенной информации, требования не передавать такую информацию третьим лицам без согласия ее обладателя. Как следует из данного определения, конфиденциальность представляет

[111] Приказ ФНС РФ от 12.12.2006 № САЭ-3-13/848@ «О проведении опытной эксплуатации унифицированной системы приема, хранения и первичной обработки налоговых деклараций и бухгалтерской отчетности в электронном виде по телекоммуникационным каналам связи» // СПС «Консультант плюс»

собой деятельность, состоящую в запрете на совершение определенных действий.

Существует ряд научно обоснованных мнений о сущности конфиденциальности информации, которые можно свести к следующим:

- конфиденциальность информации - прежде всего характеристика самой информации, ее состояния и режима, из которого вытекает требование… не передавать информацию третьим лицам[112];

- конфиденциальность информации – свойство информации[113];

- конфиденциальная информация - это информация, доступ к которой имеет ограниченный круг лиц[114] и т.д.

Здесь следует иметь в виду, что многие исследователи не придают значения тому обстоятельству, что с 2006 года следует различать понятия: «конфиденциальность информации» и «конфиденциальная информация». Последнее содержалось в тексте закона, утратившего силу в связи с принятием Федерального закона от 27.07.2006 N 149-ФЗ[115], и раскрывалось следующим образом: «конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации».

В существующей формулировке Закона Об информации нет ссылки ни на документированность информации, ни на ограничение доступа к информации.

Реакция Конституционного суда Российской Федерации по поводу конфиденциальности информации можно проследить по ряду судебных решений[116], где прослеживается переход от одной терминологии к другой.

---

[112] Право на доступ к информации. Доступ к открытой информации/ Отв. Ред.И.Ю.Богдановская._М., 2009, С. 56

[113] Королев А.Н., Плешакова О.В. Комментарий к Федеральному закону «Об информации, информационных технологиях и о защите информации». М., 2007. С. 7

[114] Серебренников М.М. Обязанность участников обществ с ограниченной ответственностью не разглашать конфиденциальную информацию общества // Правовые вопросы строительства. 2007. №

[115] Федеральный закон от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» // СЗ РФ, 20.02.1995, № 8, ст. 609

[116] Определение Конституционного Суда РФ от 18.01.2011 № 8-О-П «По жалобе открытого акционерного общества "Нефтяная компания "Роснефть" на нарушение конституционных прав и свобод положением абзаца первого пункта 1 статьи 91 Федерального закона "Об акционерных обществах»; Постановление Конституционного Суда РФ от 29.11.2010 № 20-П «По делу о проверке конституционности положений статей 20 и 21 Федерального закона "О содержании под стражей подозреваемых и обвиняемых в совершении преступлений" в связи с жалобами граждан Д.Р. Барановского, Ю.Н. Волохонского и И.В. Плотникова» и т.д.

Анализ понятия конфиденциальности информации позволяет видеть, что его элементами выступают:

- обязательные для выполнения лицом, получившим доступ к определенной информации требования не передавать такую информацию третьим лицам;

-согласие (несогласие) обладателя на передачу определенной информации третьим лицам.

Таким образом, в законодательстве определена обязанность одного субъекта и право другого субъекта, никак не взаимосвязанные с предметом правоотношения, что можно было бы связать с правовым режимом конфиденциальности информации.

В силу несовершенства законодательства не определено, какого рода информация подпадает под указанное понятие, однако, положениями ст.ст. 9, 16 Закона «Об информации» определена обязательность соблюдения конфиденциальности информации, доступ к которой ограничен федеральными законами, сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, а также соблюдение конфиденциальности информации ограниченного доступа. Таким образом: в отношении информации ограниченного доступа всегда соблюдается конфиденциальность.

Обращает на себя внимание то обстоятельство, что содержание всех правовых режимов информации содержит ряд типовых элементов:

- его целевое назначение;

- объект правового регулирования;

- правовое положение субъектов правового режима;

- комплекс способов правового регулирования и средств юридического воздействия.

Целевое назначение правового режима информации заключается в установлении прав и обязанностей субъектов по поводу информации, их защите, обеспечении информационной безопасности и баланса интересов личности, общества, государства[117].

Таким образом, конфиденциальность информации не содержит обязательные признаки правового режима информации, в связи с чем можно

[117] Терещенко Л.К. К вопросу о правовом режиме информации // Информационное право, 2008, № 1

сказать, что конфиденциальность как вид деятельности не имеет ничего общего ни с категориями (классами) информации, ни с правовым режимом информации.

Официальная классификация информации конфиденциального характера находит свое отражение в Указе Президента Российской Федерации № 188 «Об утверждении перечня сведений конфиденциального характера». [118]

В соответствии с положениями Президентского перечня информацию конфиденциального характера следует подразделять на следующие категории:

- персональные данные, к которым отнесены сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность;
- сведения, составляющие тайну следствия и судопроизводства;
- сведения о защищаемых лицах и мерах государственной защиты;
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;
- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);
- коммерческая тайна, к которой отнесены сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;
- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Несмотря на критические замечания в отношении данного Указа[119], обращает на себя внимание то обстоятельство, что до настоящего времени это

[118]Указ Президента Российской Федерации «Об утверждении перечня конфиденциального характера» № 188 от 06.03.1997 г.

[119] См., например: Лопатин В.Н. Концепция развития законодательства в сфере обеспечения информационной безопасности Российской Федерации (проект). М., 1998. С. 155; Шевердяев С.Н. Конституционно-правовой режим информации ограниченного доступа // Конституционное и муниципальное право.2007.№1; Мозолин В.П., Петровичева Ю.П. Информация и право // Журнал российского права. 2004. № 8. С. 58.

единственный нормативный акт, раскрывающий в той или иной мере структуру сведений конфиденциального характера.

Учеными предлагаются иные подходы к классификации информации ограниченного доступа, так, по мнению С.Д. Бражника следует подразделять совокупность информации по характеристике субъекта, обладающего ею, соответственно выделяя:

- личную конфиденциальную информацию, которая касается личной жизни человека (членов его семьи), его религиозных и политических убеждений и т.д., если она не известна другим лицам или не может быть ими свободно получена, в отношении которой правоспособным гражданином (членами семьи) принимаются меры по ее охране;
- конфиденциальную информацию юридических лиц, которая составляет служебную, коммерческую и банковскую тайны, исходя из того обстоятельства, что указанная информация имеет действительную и потенциальную ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель принимает меры к охране ее конфиденциальности;
- государственную конфиденциальную информацию, т. е. информацию, составляющую государственную тайну. К ней относятся сведения в военной области, и области экономики, науки и техники, внешней политики и др.

Классификация, предложенная Г. Шнейкертом включает в себя максимально большие группы информации ограниченного доступа, сформированные по признаку определенности или относительности круга лиц, владеющих тайной:

- индивидуальные, возникающие между двумя конкретными лицами или в виде знаний одного лица, секреты;
- секреты коллективные, возникающие в более широком, порой абсолютно не определенном кругу лиц;

Гайнуллина З.Ф. отмечает, что «к информации ограниченного доступа необходимо относить:[120]

- документированную информацию о государственной тайне (в порядке защиты интересов государства);

[120] См.: Гайнуллина З.Ф.Указ.соч.-С. 30.

- документированную конфиденциальную информацию, которая в свою очередь подразделяется на информацию, содержащую: а) сведения об изобретательской и предпринимательской деятельности; б) персональные данные (в порядке защиты личной тайны)».

Сразу обращает на себя внимание, что недостатком данного подхода является возможность классификации лишь некоторых из категорий информации ограниченного доступа, при этом классификация затрагивает только документированную информацию.

Классификация, предлагаемая В.Б. Веховым указывает на следующие виды защищаемой информации:

- сведения, отнесенные к государственной тайне;
- сведения, отнесенные к служебной и коммерческой тайне;
- сведения, имеющие статус персональных данных.

Л.А. Шиверский, опираясь на нормы действующего законодательства, проводит градацию тайны исходя из грифа секретности, причем для сведений, составляющих государственную тайну, устанавливаются три степени секретности и соответствующие этим степеням грифы секретности для носителей указанных сведений; «особой важности», «совершенно секретно» и «секретно». Для иных видов конфиденциальной информации автор предлагает к использованию грифы «конфиденциально», «для служебного пользования».

Отталкиваясь от характеристики обладателя сведений, И.В. Смолькова, выделяет следующие виды информации ограниченного доступа:[121]

- государственная тайна;
- личная тайна;
- семейная тайна;
- профессиональная тайна, которая подразделяется на тайны:
  - в чистом виде, обусловленная характером деятельности (служебная, коммерческая);
  - составную часть которой образуют доверенные личные тайны граждан (адвокатская, врачебная).

Помимо изложенного, существует также ряд классификаций, основанных на сущности информации, составляющей тайну, позволяющих определить, каким

[121] См.: Смолькова И.В. Проблемы охраняемой законом тайны в уголовном процессе. -М.: Луч, 1999.-С. 13; Смолькова И.В. Тайна и уголовно- процессуальный закон. - М.: Луч, 1997.-С.6; Смолькова И.В. Частная жизнь граждан: основания и пределы процессуального вмешательства.- М.: Луч,- 1997. - С.36.

субъектам общества будет нанесен ущерб в случае обнародования той или иной закрытой информации:

- тайна частной жизни (банковская, врачебная, тайна переписки, нотариальная, тайна усыновления, страхования, исповеди, голосования);
- коммерческая тайна и различные конфиденциальные данные (коммерческая, журналистская, редакционная тайны);
- государственные секреты (государственная и служебная тайна).

С.В. Кузьмин предлагает проводить классификацию тайны по критериям характера общественных отношений, возникающих по поводу интересов охраны той или иной тайны в связи с интересами: [122]

- конституционных и иных прав личности (личная тайна);
- семейной жизни (семейная тайна усыновления);
- предпринимательской деятельности (коммерческая и банковская тайна);
- безопасности государства (государственная тайна);
- государственной службы и службы в органах местного самоуправления (должностная служебная тайна);
- службы в коммерческих и иных организациях (иная служебная тайна);
- предварительного расследования (следственная тайна);
- с нормальным отправлением правосудия и осуществлением предварительного следствия (свидетельская тайна);
- безопасности субъектов порядка управления (тайна безопасности субъектов порядка управления).

В качестве дополнительного фактора предлагается рассматривать признак законодательной техники, подразделяемой на непосредственнаую, когда указание на охрану которой содержится в нормах права; и опосредованную - прямое указание на которую в тексте правовой нормы отсутствует, но тайна имеет правовое значение в силу предписания иных актов федерального законодательства или норм международного права.

В.В. Крыловым предложена классификация, основанная на законодательном установлении о том, что в Российской Федерации существует право собственности граждан, юридических лиц и государства, что позволяет определять режим использования различных видов информации. По его мнению, действующим законодательством установлена защита нескольких

[122] См.: Кузьмин С.В. Указ. соч. -С. 8.

видов информации, принадлежащей гражданам (личной конфиденциальной информации), к которой, в частности, относятся:

- коммуникационные тайны (тайна переписки, телефонных переговоров, почтовых телеграфных или иных сообщений (ч. 2 ст. 23 Конституции РФ; ст. 138 УК РФ);
- тайна усыновления (ст. 155 УК РФ; ст. 39 Семейного кодекса РФ);
- сведения о частной жизни лица (ст. 137 УК РФ; ст. 150 ГК РФ);
- личная тайна (ст. 137 УК РФ; ст. 150 ГК РФ);
- семейная тайна (ст. 137 УК РФ; ст. 150 ГК РФ);
- тайна голосования (ст. 142 УК РФ);
- информация, являющаяся объектом авторских и смежных прав (Закон РФ от 9 июля 1993 г. «Об авторском праве и смежных правах»[123]; ст. 146 УК РФ; ст. 150 ГК РФ);
- информация, непосредственно затрагивающая права и свободы гражданина или персональные данные (Закон РФ от 20 февраля 1995 г. «Об информации, информатизации и защите информации[124]; ст. 140 УК РФ);
- профессиональная тайна (нотариальная тайна, адвокатская тайна, медицинская (врачебная) тайна).

Позиция В.М. Михайлова[125] основывается на том, что Конституция РФ, с одной стороны, - закрепляет право граждан, организаций и государства на тайну, но, в то же время, действующее законодательство гарантирует и другое важнейшее право - свободно искать, получать, передавать, производить и распространять информацию любым законным способом, что позволяет объединить все виды тайн в три основные группы:

- сведения, составляющие тайну частной жизни: банковская тайна (тайна вкладов); врачебная (медицинская) тайна; тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; тайна предварительного следствия; нотариальная тайна; тайна усыновления; тайна страхования; адвокатская тайна; тайна исповеди; тайна голосования; сведения о мерах безопасности судей, должностных лиц правоохранительных и контролирующих органов.

[123] В настоящее время правовое регулирование в сфере авторского права осуществляется положениями ч.4 Гражданского кодекса Российской Федерации.
[124] В настоящее время утратил силу
[125] Михайлов В.М. Право па тайну. // Закон. - 1998. - № 2. - с. 24-28,

- сведения, составляющие коммерческую тайну, а также иные конфиденциальные данные, связанные с экономической деятельностью (в т.ч. журналистская и редакционная тайна).
- государственные секреты, включающие: государственную тайну; служебную тайну; иную служебную информацию.

Сусловой С.И. предлагается следующая классификация:

- частные тайны, к которым относятся сведения, содержащие в чистом виде личную и семейную тайны (тайна жилища, тайна личных записей, тайна почтовой корреспонденции, тайна голосования), а также конфиденциальные сведения о личности, полученные субъектом в связи с осуществлением его профессиональной деятельности (тайна усыновления, тайна исповеди, медицинская, банковская тайны);

- тайны организаций, предприятий, учреждений, включающие в себя сведения, составляющие служебную тайну (тайна следствия и судопроизводства, в том числе тайна совещания судей, тайна внутреннего административного делопроизводства), а также сведения, относящиеся к коммерческой тайне;

- государственные тайны, к которым относятся: сведения в военной в области экономики, науки и техники, сведения в области внешней политики и экономики, сведения в области разведывательной, контрразведывательной и оперативно - розыскной деятельности.

Некоторые виды тайн носят смешанный характер. Так тайна следствия включает обязанность сохранения профессиональных тайн и доверенных личных тайн граждан, а адвокатская тайна может состоять из личных тайн граждан, служебных тайн предприятий, государственных тайн.

Как следует из представленных классификаций, в их основу положена либо категория информации, либо характеристика субъекта.

Анализируя предлагаемые способы классификации информации ограниченного доступа, обращает на себя внимание то обстоятельство, что исследователями уделяется незначительное внимание проблематике режима тайны.

Так, следует иметь в виду, что Законами «О государственной тайне» и «О коммерческой тайне» максимально регламентирован комплекс мероприятий, направленных на обеспечение защиты сведений, составляющих указанные

категории информации ограниченного доступа, в ходе которых максимально регламентирован следующий круг вопросов[126]:

- определен перечень сведений, составляющих, а главное, не могущих составлять государственную и коммерческую тайну;

- определен круг органов, осуществляющих защиту государственной и коммерческой тайны и пределы их полномочий;

- установлен порядок отнесения сведений к государственной и коммерческой тайне, порядок засекречивания и рассекречивания сведений и их носителей;

- указаны реквизиты носителей сведений, составляющих данные категории тайны;

- определены порядок допуска лиц к указанным категориям сведений, а также порядок предоставления сведений, составляющих государственную и коммерческую тайну.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»[127] в значительной мере посвящен режиму персональных данных, именно как комплексу мер по их охране, к чему отнесены принципы, условия и особенности обработки персональных данных, их категории, условия трансграничной передачи персональных данных, права и обязанности субъектов обработки. К сожалению, в указанном законе дается достаточно расплывчатое понятие персональных данных как любой информации, относящаяся к определенному или определяемому на основании такой информации физическому лицу, что создает дополнительную проблематику в практике применения указанного закона.[128]

Следует также иметь в виду, что существуют некоторые категории тайн, содержание которых раскрывается законодателем достаточно подробно, однако меры по охране указанной информации ограниченного доступа – не определен. К указанным тайнам можно отнести, в частности:

---

[126] Беспалов Д.Н., Елин В.М. Правовой режим государственной тайны как пример правового режима информации ограниченного доступа // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016. № 3-4. С. 127-136.

[127] Федеральным законом № 152-ФЗ «О персональных данных» от 27.07.2006 // СЗ, 31.07.2006, № 31 (1 ч.), ст. 3451

[128] *См., например: Бундин М.В.* Персональные данные как термин российского законодательства // Правовые вопросы связи, 2009, № 1; *Косякин А.В.* Административная ответственность за нарушение законодательства о персональных данных //Административное и муниципальное право, 2009, № 3

- аудиторскую тайну, которую составляют любые сведения и документы, полученные и (или) составленные аудиторской организацией и ее работниками, а также индивидуальным аудитором и работниками, с которыми им заключены трудовые договоры, при оказании услуг, предусмотренных настоящим Федеральным законом, за исключением сведений разглашенных самим лицом, которому оказывались услуги, предусмотренные настоящим Федеральным законом, либо с его согласия; о заключении с аудируемым лицом договора о проведении обязательного аудита; о величине оплаты аудиторских услуг[129];

- банковскую тайну об операциях, о счетах и вкладах клиентов и корреспондентов[130];

- врачебную тайну, т.е. информацию о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении[131];

- налоговую тайну как любые полученные налоговым органом, органами внутренних дел, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений, определенных п.п. 1-5 ч.1 ст. 102 НК РФ132. Что характерно, ч.3 указанной статьи определено, что поступившие в налоговые органы, органы внутренних дел, органы государственных внебюджетных фондов или таможенные органы сведения, составляющие налоговую тайну, имеют специальный режим хранения и доступа, однако особенности указанного специального режима нормативными актами на раскрываются.

Дополнительную сложность рассматриваемому вопросу придает то обстоятельство, что содержание значительного количества хорошо известных и достаточно распространенных тайн законодательно не раскрывается. Для понимания сущности возникающей при этом проблемы достаточно рассмотреть пример широко распространенной тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, правовой режим которой определен ч. 2 ст. 23 Конституции РФ.

---

[129] Ст.9 Федерального закона «Об аудиторской деятельности» от 30.12.2008 № 307-ФЗ // СЗ РФ, 05.01.2009, № 1, ст. 15

[130] Ст.26 Федерального закона «О банках и банковской деятельности» закон от 02.12.1990 № 395-1 // СЗРФ 05.02.1996, № 6, ст. 492

[131] Ст.61 Основ законодательства Российской Федерации об охране здоровья граждан // Ведомости СНД и ВС РФ, 19.08.1993, № 33, ст. 1318

[132] Ст. 102 Налогового кодекса Российской Федерации // СЗ РФ, № 31, 03.08.1998, ст. 3824

Значимость указанной категории информации ограниченного доступа определена В.Н.Лопатиным, определившего объектом права неприкосновенность частной жизни каждого гражданина[133], относя тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений к правам на тайну личной жизни.

Характеризуя указанную категорию тайн, В.Н. Лопатин ссылается на решение Европейского Суда по правам человека по пониманию и применению Европейской Конвенции о защите прав человека и основных свобод, согласно которому: "существование определенного законодательства, разрешающего вести скрытое наблюдение за почтой и связью, является, ввиду исключительных условий, необходимым в демократическом обществе". Определяя критерии правомерности подслушивания Европейский суд указал, что вмешательство не противоречит требованиям Конвенции, если:

- оно предусмотрено законом и необходимо в демократическом обществе в интересах государственной безопасности, общественного порядка или экономического благосостояния страны, в целях предотвращения беспорядка или преступлений, охраны здоровья или защиты нравственности или защиты прав и свобод других лиц;

- осуществляется в соответствии с законом;

- закон и принятые на его основе подзаконные акты известны общественности и легкодоступны;

- нормативные акты носят настолько четкий и определенный характер, что, исходя из них, заинтересованные лица могут корректировать свое поведение;

- в них фиксируются пределы компетенции государственных органов, уполномоченных принимать решения о подслушивании и осуществлять его, и ограничения на способы реализации этих правомочий;

- вмешательство необходимо для защиты демократических ценностей и институтов;

- оно осуществляется в целях предотвращения и пресечения не каких-то мелких, а вполне определенных и наиболее опасных преступлений;

[133] Лопатин В.Н. Защита права на неприкосновенность частной жизни // Журнал российского права, № 1, 1999

- круг лиц, против которых предпринимаются означенные действия, строго ограничен;

- подслушивание носит выборочный, а не общепоисковый характер;

- обеспечивается институализированный контроль за принятием решений о подслушивании, самим подслушиванием и его прекращением;

- вмешательство рассматривается как временная мера;

- в отношении информации, полученной в результате прослушивания телефонных разговоров, применяется правило конфиденциальности;

- в случае прекращения преследования или оправдания по требованию соответствующего лица записи либо возвращаются ему, либо уничтожаются.

В отношении указанной категории информации осуществляется уголовно – правовая защита, предусматривающая уголовную ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан по ч.1 ст. 138 УК РФ.

По мнению Д.О.Феоктистова диспозиция ч. 1 ст. 138 УК РФ носит бланкетный характер и требует знания многих иных нормативных актов.[134] При этом тайна переписки, почтовых, телеграфных и иных сообщений в специальной литературе называется тайной связи и определяется как входящая в сферу деятельности операторов почтовой связи, не подлежащая разглашению без согласия пользователя услуг почтовой связи.

Между тем, статьей 63 Федерального закона «О связи»[135] определено, что на территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, причем сохранение тайны связи является обязанностью оператора.

Статья 15 Федерального закона «О почтовой связи»[136] определяет, что тайна переписки, почтовых, телеграфных и иных сообщений, входящих в сферу деятельности операторов почтовой связи, гарантируется государством. При этом к тайне связи отнесена информация об адресных данных пользователей услуг почтовой связи (персональные данные – прим. авт.), о почтовых отправлениях, почтовых переводах денежных средств,

[134] Феоктистов Д.О. Особенности состава преступления, предусмотренного ст. 138 УК РФ // Международное публичное и частное право, 2007, № 1

[135] Федеральный закон «О связи» // СЗ РФ, 14.07.2003, № 28, ст. 2895

[136] Федеральный закон «О почтовой связи» // СЗ РФ, 19.07.1999, № 29, ст. 3697

телеграфных и иных сообщениях, входящих в сферу деятельности операторов почтовой связи, а также сами эти почтовые отправления, переводимые денежные средства, телеграфные и иные сообщения.

Таким образом, можно сделать вывод о том, что, несмотря на предпринимаемые законодателем ряд попыток раскрыть содержание данной категории информации, сформировать полное представление о ней на основании нормативных актов представляется достаточно проблематичным.

Несомненно, существует значительное количество научной и специальной литературы, посвященной вопросам отнесения тех или иных сведений к различным категориям тайн, однако указанные исследования не находят своего отражения в практической деятельности.

Таким образом, можно сделать вывод о том, что дополнительную категорию тайн составляют сведения, содержание которых не раскрывается (или раскрывается в недостаточном объеме), к которым, в частности можно отнести:

- тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений;

- тайну связи, т.е. информацию об адресных данных пользователей услуг почтовой связи, о почтовых отправлениях, почтовых переводах денежных средств, телеграфных и иных сообщениях, входящих в сферу деятельности операторов почтовой связи, а также сами эти почтовые отправления, переводимые денежные средства, телеграфные и иные сообщения; [137]

- тайну страхования - сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц138;

- тайну завещания - сведения, касающиеся содержания завещания, его совершения, изменения или отмены139;

- тайну исповеди – обстоятельства, ставшие известными священнослужителю из исповеди140;

- тайна усыновления141, и т.д.

---

[137] Ст. 15 Федерального закона «О почтовой связи» от 17.07.1999 № 176-ФЗ // СЗ РФ, 19.07.1999, № 29, ст. 3697

[138] Ст. 946 ГК РФ

[139] Ст. 1123 ГК РФ

[140] Ст. 56 УПК РФ; Федеральный закон «О свободе совести и о религиозных объединениях» от 26.09.1997 № 125-ФЗ // СЗ РФ, 29.09.1997, № 39, ст. 4465

[141] Ст. 139 СК РФ

Указанное позволяет ввести дополнительную классификацию сведений, составляющих тайну, по установленным в отношении них режимам защиты информации, подразделяя на:

- тайны с установленным по их охране режимом, к которым следует относить государственную и коммерческую тайну;
- тайны с частично установленным режимом, к которым следует относить, в частности, персональные данные;
- тайны с неопределенным режимом защиты информации;
- тайны с неопределенным характером сведений, образующих данную категорию информации ограниченного доступа.

Дополнительно следует отметить проблему устойчивости режима защиты информации к внешним воздействиям.

При этом, характеризуя внешние воздействия их можно подразделить в первую очередь на законные и незаконные.

Так, классифицируя информацию ограниченного доступа с точки зрения организации защиты сведений ограниченного доступа, определения пределов вмешательства и круга посвященных субъектов, С.И.Суслова предлагает классификацию тайн в зависимости от возможности допуска к этой информации:

- тайны с режимом абсолютного запрета на вмешательство, в отношении которых законом не предусматривается возможность требования от их владельцев (обладателей) допуска к этой информации. Эти тайны не должны оглашаться даже в суде, если на то не будет разрешения их владельца или обладателя (тайна исповеди, тайна голосования, адвокатская тайна, тайна совещания судей, донорская тайна, тайна депутата, тайна усыновления);
- тайны с законодательно установленным режимом ограниченного допуска, режим которых определен законодателем: в федеральных законах закреплены права их владельцев, обладателей, их обязанности, предусмотрен порядок предоставления этой информации третьим лицам. Для посвящения в нее необходимо преодолеть какие-либо рубежи защиты (коммерческая тайна, государственная тайна);
- тайны с режимом индивидуальной защиты – защищены от широкой огласки, но передача этой информации не требует исполнения особых

процедур и часто является обязанностью участников уголовного процесса (некоторые сведения о частной жизни граждан).

Анализируя положения Указа № 188 также обращает на себя внимание то обстоятельство, что в настоящее время не существует нормативного определения понятия «служебная тайна», поскольку основы действующего правового режима служебной тайны были урегулированы в Гражданском кодексе РФ в одной статье с коммерческой тайной (ст. 139 ГК)[142].

По всей видимости, это означало очевидное единство основных нормативных установок служебной и коммерческой тайн, однако обоснованность этого шага уже давно беспокоила цивилистов: «...вызывает сомнение правомерность распространения условий охраны коммерческой тайны на служебную информацию. Это разноплановые понятия. Различны и основания, по которым сведения, относящиеся к служебной тайне, и сведения, составляющие коммерческую тайну, признаются конфиденциальными. Сохранение в тайне служебной информации не обусловлено ее коммерческой ценностью (хотя такая информация и может содержать сведения коммерческого характера). Служебная тайна не может быть объектом гражданского оборота. Запрещение ее разглашать, как правило, основывается на законодательстве, регламентирующем отдельные виды деятельности, затрагивающей в т.ч. сферу частной жизни гражданина[143]. Определенные категории работников, занимающихся такой деятельностью, обязаны сохранять в тайне сведения, к которым они имеют доступ в связи с выполняемой работой (банковские служащие, работники связи, налоговые инспекторы, страховые агенты, врачи и др.)»[144].

---

[142] Формулировка Статьи 139 Гражданского кодекса Российской Федерации «Служебная и коммерческая тайна» определяла, что «Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.
2. Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами.
Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.»

[143] См., например, ст. 33 Федерального закона от 27 ноября 1992 г. № 4015-1 «Об организации страхового дела в Российской Федерации», ст. 63 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи».

[144] См.: Комментарий к Гражданскому кодексу РФ, части первой (постатейный) / Отв. ред. О.Н. Садиков. М., 2005.

Следует также различать служебную и коммерческую тайну, поскольку, по мнению В.А. Дозорцева: «Критерием служебной информации служит основание необщедоступности - трудовое законодательство и заключенный на его основе трудовой договор, служебные отношения, когда работодатель устанавливает обязанность работника соблюдать конфиденциальность. А основанием для конфиденциальности коммерческой информации является ее содержание - действительная или потенциальная коммерческая ценность в силу ее неизвестности третьим лицам»[145].

Таким образом, сформулировано мнение о том, что служебную тайну могут образовывать сведения, находящиеся в распоряжении органов власти и подпадающие под правовой режим конфиденциальной информации. При этом выделяется два вида сведений, которые относятся к служебной тайне органов власти: во-первых, это собственная тайна органа власти, представляющая собой оригинальную охраноспособную информацию, выработанную самим органом власти, во-вторых, это тайна других лиц, т.е. конфиденциальные сведения о гражданах и организациях, собранные органом власти в процессе реализации установленных для него полномочий. Так, органы власти отвечают за сохранность полученных на законном основании сведений о частной жизни лица, сведений, составляющих коммерческую тайну, профессиональную тайну (врачебную, нотариальную, тайну усыновления), и т.д.

Различие правовых режимов коммерческой и служебной тайны было отчасти подтверждено развитием текущего законодательства, однако неопределенность здесь продолжала сохраняться. Федеральный закон[146] упоминал о служебной тайне только в одном отношении - когда требовалось обеспечить конфиденциальность коммерческой тайны, в случае если она на законном основании оказывалась в распоряжении органов власти, т.е. когда коммерческая тайна, условно говоря, превращалась в органах власти (и только для них) в служебную тайну (ст. 13). В этом смысле важно обратить внимание на замечание О.С. Соколовой, что при передаче в органы власти охраноспособной информации происходит не трансформация режимов, а

[145] См.: Дозорцев В.А. Интеллектуальные права: Понятие. Система. Задачи кодификации. Сб. статей. М., 2005. С. 132.

[146] См.: Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ (в ред. Федерального закона от 2 февраля 2006 г. № 19-ФЗ)

«возникновение множественности отношений по поводу одного и того же вида информации, ведь в органы исполнительной власти предоставляется не режим, а сама информация»[147]. Иными словами, обладание одной и той же информацией разными субъектами порождает для них разные права и обязанности, т.е. информация может иметь множественный правовой режим.

2.2. Гражданско-правовые механизмы обеспечения информационной безопасности

При определении возможности использования гражданско-правового инструментария обеспечения информационной безопасности, следует учесть специфику субъективного права на защиту в гражданском праве, по поводу которой существует по крайней мере две точки зрения[148]:

- право на защиту является самостоятельным субъективным правом;

- право на защиту можно рассматривать как юридически закрепленную возможность управомоченного лица использовать меры правоохранительного характера с целью восстановления нарушенного права и пресечения действий, нарушающих право[149].

Способы защиты гражданских прав подразделяются на меры государственно-принудительного порядка, обладающие признаками мер гражданско-правовой ответственности, и на меры защиты в узком смысле слова, не обладающие признаками гражданско-правовой ответственности[150]. К мерам гражданско-правовой ответственности следует относить: возмещение убытков (вреда), взыскание неустойки и имущественную компенсацию морального вреда. Все остальные меры защиты гражданских прав именуются мерами защиты гражданских прав в узком смысле слова.

Существующая специфика гражданско-правового обеспечения информационной безопасности связана с неопределенностью статуса

---

[147] См.: Соколова О.С. Административно-правовые режимы конфиденциальной информации в системе специальных административно-правовых режимов // Современное право. 2005. № 8. С. 40.

[148] Братусь С.Н. Юридическая ответственность и законность. М., 1976. С. 72 - 79.

[149] Российское гражданское право: В 2 т. Общая часть. Вещное право. Наследственное право. Интеллектуальные права. Личные неимущественные права: Учебник (том 1) // отв. ред. Е.А. Суханов. М., 2011. С. 190

[150] Красавчиков О.А. Ответственность, меры защиты и санкции в советском гражданском праве // Категории науки гражданского права: Избранные труды: В 2 т. (серия "Классика российской цивилистики"). Т. 2. М., 2005. С. 257 - 262.

информации как объекта гражданско - правовых отношений. С принятием нового гражданского кодекса Российской Федерации информация была включена в перечень объектов гражданских правоотношений, определенный ст. 128 ГК РФ и входила в их число до 01 января 2008 года, когда с вступлением в силу ч.IV ГК РФ информация была исключена из содержания ст. 128 КГ РФ. Таим образом правоотношения, объектом которых выступала информация, были законодательно исключены из правого пространства одновременно с дополнением законодательства нормами ч.IV ГК РФ, которая связана с результатами интеллектуальной деятельности и приравненными к ним средствами индивидуализации.

Таким образом, в настоящее время сложилась парадоксальная ситуация:

- гражданско-правовое регулирование оборота информации подменено регулированием правоотношений в сфере прав на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации;

- информация не имеет собственника или обладателя. В отношении результатов интеллектуальной деятельности применяется понятие «правообладатель», под которым понимается гражданин или юридическое лицо, обладающие исключительным правом на результат интеллектуальной деятельности или на средство индивидуализации;

- имеет место собственник информации, отнесенной к государственной тайне, под которым понимается предприятие, учреждение, организация или гражданин, имеющий в собственности информацию данной категории, причем о данной категории лиц сложно сказать что-то определенное;

- существует прямой запрет для результатов интеллектуальной деятельности и приравненных к ним средствам индивидуализации на возможность отчуждения или перехода иными способами от одного лица к другому;

- в случаях и в порядке, которые установлены ГК РФ, права на результаты интеллектуальной деятельности и средства индивидуализации, а также материальные носители, в которых выражены соответствующие результаты или средства, могут отчуждаться или иными способами переходить от одного лица к другому;

- информация не может быть объектом гражданских отношений, поскольку «выпала» из системы правового регулирования, сделки в отношении информации никак не регулируются, они «выпали» из правового пространства;

- информационное право не охватывает данную сферу, поскольку принципиально дистанцируется от гражданских правоотношений, регулируя отношения, возникающие при: осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации[151].

Если исходить из того, что на смену информации как объект гражданско-правовых отношений пришли права на результаты интеллектуальной деятельности и средства индивидуализации, то следует иметь в виду, что ст. 1225 ГК РФ подразделяет их на 16 категорий.

Ст. 1226 ГК РФ определяет, что на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации признаются интеллектуальные права, которые включают личные неимущественные права, исключительное право, являющееся имущественным правом и иные права (право следования, право доступа и другие).

С личными неимущественными правами и другими нематериальными благами, принадлежащими гражданину от рождения или в силу закона, связаны нематериальные блага, к которым, в свою очередь, относятся: жизнь и здоровье, достоинство личности, личная неприкосновенность, честь и доброе имя, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна, право свободного передвижения, выбора места пребывания и жительства, право на имя, право авторства.

Особенностью личных неимущественных прав и другие нематериальных благ, принадлежащих гражданину от рождения или в силу закона, выступает их неотчуждаемость и непередаваемость иным способом. В силу ст. 1251 ГК РФ в случае нарушения личных неимущественных прав автора их защита осуществляется, в частности, путем признания права, восстановления положения, существовавшего до нарушения права, пресечения действий,

---

151

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗРФ, 31.07.2006, № 31 (1 ч.), ст. 3448

нарушающих право или создающих угрозу его нарушения, компенсации морального вреда, публикации решения суда о допущенном нарушении.

При нарушении личных неимущественных прав в первую очередь встает вопрос о возмещении морального вреда.

Под моральным вредом понимаются[152] нравственные или физические страдания, причиненные действиями (бездействием), посягающими на принадлежащие гражданину от рождения или в силу закона нематериальные блага (жизнь, здоровье, достоинство личности, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна и т.п.), или нарушающими его личные неимущественные права (право на пользование своим именем, право авторства и другие неимущественные права в соответствии с законами об охране прав на результаты интеллектуальной деятельности) либо нарушающими имущественные права гражданина. Степень нравственных или физических страданий оценивается судом с учетом фактических обстоятельств причинения морального вреда, индивидуальных особенностей потерпевшего и других конкретных обстоятельств, свидетельствующих о тяжести перенесенных им страданий.

В настоящее время вопросы возмещения морального вреда, в частности, регулируются ст.ст. 150-152, 1099-1101 ГК РФ; ст.15 Закона Российской Федерации от 7 февраля 1992 г. «О защите прав потребителей»; ч. 5 ст. 18 Федерального закона «О статусе военнослужащих»; ст. 237 ТК РФ; п. 3 ст. 8 Федерального закона «Об обязательном страховании от несчастных случаев на производстве и профессиональных заболеваний»; п. 2 ст. 38 Федерального закона от 13 марта 2006 г. «О рекламе»[153].

Согласно положениям ст. 1251 ГК РФ, в случае нарушения личных неимущественных прав автора их защита осуществляется, в частности, путем признания права, восстановления положения, существовавшего до нарушения права, пресечения действий, нарушающих право или создающих угрозу его нарушения, компенсации морального вреда, публикации решения суда о допущенном нарушении.

Исключительность имущественных прав на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации связан с тем

[152] Постановление Пленума Верховного Суда РФ от 20.12.1994 № 10 (ред. от 06.02.2007) «Некоторые вопросы применения законодательства о компенсации морального вреда» // РГ, № 29, 08.02.1995

[153] В ред. Постановления Пленума Верховного Суда РФ от 06.02.2007 № 6

обстоятельством, что в законе существует прямой запрет для неправомочных лиц на возможность использовать эти интеллектуальные продукты, т.е. "исключает" для этих "других" такую возможность[154].

При этом в полной мере прослеживается постулат о том, что о том, «в рынке интеллектуального продукта выступает не сам продукт, а права на него. Вне прав такой продукт, являющийся нематериальным, выступать на рынке не может»[155]. При этом осуществляется защита имущественных (исключительных) и личных неимущественных прав. Раскрывая назначение защиты прав на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации, обращает на себя достаточно единообразный подход к характеристике ее целей и задач, к которым российскими авторами отнесено:

- защита личных неимущественных прав и интересов, выражающаяся в соблюдении прав на авторство, на имя, на неприкосновенность произведения и т.д.;

- имущественный интерес, выражающийся в возможности получать вознаграждение за труд;

- общественный интерес, выражающийся в возможности приумножения культурного и научного общественного достояния

Ст. 1252 ГК РФ определено, что защита исключительных прав на результаты интеллектуальной деятельности и на средства индивидуализации осуществляется, в частности, путем предъявления требования:

- о признании права;

- о пресечении действий, нарушающих право или создающих угрозу его нарушения;

- о возмещении убытков;

- об изъятии материального носителя в соответствии с решением суда;

- о публикации решения суда о допущенном нарушении с указанием действительного правообладателя.

Ст. 1225 ГК РФ напрямую относит к результатам интеллектуальной деятельности программы для электронных вычислительных машин

---

[154] Маковский А.Л. Исключительные права и концепция части четвертой Гражданского кодекса // Гражданское право современной России / Сост. О.М. Козырь и А.Л. Маковский. М.: Статут, 2008. С. 103 - 141.

[155] Дозорцев В.А. Интеллектуальные права. Понятие. Система. Задачи кодификации. М., 2003. С. 59

(программы для ЭВМ) и базы данных. Согласно ст.10 TRIPS[156] компьютерные программы (исходный текст и объектный код) охраняются как литературные произведения в соответствии с Бернской конвенцией (1971 г.). Компиляции данных или другая информация в машиночитаемой или в другой форме, которые по причине отбора или классификации своего содержания составляют результат творчества, должны охраняться как таковые.

Российской гражданское право под программой для ЭВМ понимает представленную в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.[157] Программа для ЭВМ охватывает совокупность команд на языке программирования, алгоритм работы программы, который может быть использован для различных программ. Аудиовизуальные отображения включают как аудиовизуальные произведения, то есть зафиксированные серии связанных между собой кадров (с сопровождением или без сопровождения их звуком), предназначенные для зрительного и слухового восприятия с помощью соответствующих технических средств (п. 1 ст. 1263 ГК), так и отдельные неподвижные изображения на экране монитора.

Базой данных является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ)[158]. Авторские права на осуществленные подбор или расположение материалов (составительство) принадлежат автору.

Следует иметь в виду, что согласно п. 5 ст. 1259 ГК правовая охрана не распространяется на идеи и принципы, лежащие в основе программы для

---

[156] "Соглашение по торговым аспектам прав интеллектуальной собственности" (ТРИПС/TRIPS) (Заключено в г. Марракеше 15.04.1994) // Консультант плюс

[157] Статья 1261 ГК РФ. Программы для ЭВМ

[158] Жарова А.К. Электронные формы разрешения конфликтов в сфере судебной деятельности // Российское правосудие. 2013. № 8 (88). С. 53-59.

ЭВМ или какого-либо их элемента, в том числе на идеи и принципы организации интерфейса (взаимодействие программы и самого компьютера) и алгоритма (математическое обеспечение программы), а также языки программирования. Объектом охраны выступает программа как совокупность данных и команд, которая пишется на одном из языков программирования и которая может быть зафиксирована на носителях, и подготовительные материалы.

Правообладатель в течение срока действия исключительного права на программу для ЭВМ или на базу данных может по своему желанию зарегистрировать такую программу или такую базу данных в федеральном органе исполнительной власти по интеллектуальной собственности.

Федеральным органом исполнительной власти, осуществляющим нормативно-правовое регулирование в сфере интеллектуальной собственности, определяется порядок государственной регистрации программ для ЭВМ и баз данных[159].

При этом проверяется соблюдение формальных требований, без производства экспертизы по существу. Однако, по мнению С.П.Гришаева [160] преимуществом такой регистрации является то, что она является официальным уведомлением о своих правах в отношении данного объекта и одновременно выполняет роль оперативной рекламы, причем в случае возникновения спора депонированные экземпляры могут рассматриваться судом в качестве доказательства.

По российскому законодательству программы для ЭВМ не являются изобретениями, однако могут быть включены в том или ином сочетании в состав единой технологии, которая служит технологической основой определенной практической деятельности в гражданской или военной сфере.

Европейская патентная конвенция в число перечней объектов, не считающихся изобретениями (ст. 52(2)), включила программы для электронно-вычислительных машин как таковые. При этом Конвенция определяет правовую охрану изобретений, связанных с программами для

[159] Приказ Минобрнауки РФ от 29.10.2008 № 324 «Об утверждении Административного регламента исполнения Федеральной службой по интеллектуальной собственности, патентам и товарным знакам государственной функции по организации приема заявок на государственную регистрацию программы для электронных вычислительных машин и заявок на государственную регистрацию базы данных, их рассмотрения и выдачи в установленном порядке свидетельств о государственной регистрации программы для ЭВМ или базы данных» (Зарегистрировано в Минюсте РФ 17.12.2008 № 12893) // Консультант плюс

[160] Гришаев С.П. Программы для ЭВМ по новому законодательству РФ

ЭВМ в соответствии с дополнительно директивой по проведению экспертизы в Европейском патентном бюро (ЕПВ) (с-IV, 2.3). Так, программа для ЭВМ, являющаяся предметом притязаний как таковая, или ее запись на носителе не признается изобретением несмотря на ее содержание. В то же время предмету притязаний нельзя отказать в патентоспособности лишь потому, что при его осуществлении программа для ЭВМ играет определенную роль. Если предмет притязаний вносит вклад в уровень техники, он не исключается из категории патентоспособных. Если программа в комбинации с ЭВМ изменяет способ функционирования последней, принося этим технический эффект, то такая комбинация может быть патентоспособной[161].

При этом в Европе существует практика,[162] когда программы патентуются как элементы изобретения. Подобные патенты стали выдаваться Европейским патентным ведомством (ЕПВ), и к началу 2000-х годов было выдано, по приблизительным оценкам, примерно 30000 программных патентов. Иногда тексты заявок, подаваемых разработчиками в Европейское патентное ведомство, совпадали с теми заявками, которые были поданы в США. Но практика выдавать программные патенты не всегда находила поддержку в национальных судах стран ЕС. Имелись случаи признания патентов недействительными.

Европейский парламент в июле 2005 г. отказался от одобрения директивы, которая прямо санкционировала бы выдачу патентов на компьютерно-реализованные изобретения (computer-implemented inventions), т.е. изобретения, работающие с помощью компьютерной программы, что не повлияло на практику Европейского патентного ведомства.

В США прецедентным является решение Верховного суда по делу Diamond vs Diehr[163], 450 U.S. 175 (1981) который указал, что «Математическая формула как таковая не защищается по нашим патентным законам. Если заявка касается математической формулы (или научного принципа, или природного явления), должно быть произведено исследование, не испрашивается ли по заявке патентная защита такой

[161] www.патика.ru
[162] Слыщенков В.А., Левин А.Е. Охрана программ для ЭВМ: в поисках эффективных правовых решений // Юрист", 2008, № 8
163 DIAMOND v. DIEHR, (1981). United States Supreme Court. No. 79-1112.Argued: October 14, 1980 Decided: March 3, 1981 // http://caselaw.findlaw.com/us-supreme-court/450/175.html

формулы, взятой абстрактно. Заявка отвечает требованиям, если содержит применения математической формулы либо применяет такую формулу в системе или процессе, который, взятый в целом, выполняет функцию, для защиты которой и созданы патентные законы (например, переработка или превращение предмета в иное состояние или вещь)».

Обращает на себя внимание то обстоятельство, что при этом патентуется не текст программы, а именно определенное оригинальное технологическое решение конкретной задачи, использующий программу для ЭВМ в качестве компонента.

Автору или иному правообладателю принадлежит исключительное право использовать произведение, что включает в себя:

- воспроизведение произведения, то есть изготовление одного и более экземпляра произведения или его части в любой материальной форме;
- распространение произведения путем продажи или иного отчуждения его оригинала или экземпляров;
- публичный показ произведения, то есть любая демонстрация оригинала или экземпляра произведения;
- импорт оригинала или экземпляров произведения в целях распространения;
- прокат оригинала или экземпляра произведения;
- публичное исполнение произведения, то есть представление произведения в живом исполнении или с помощью технических средств (радио, телевидения и иных технических средств);
- сообщение в эфир, то есть сообщение произведения для всеобщего сведения (включая показ или исполнение) по радио или телевидению (в том числе путем ретрансляции);
- переработка произведения, причем под переработкой (модификацией) программы для ЭВМ или базы данных понимаются любые их изменения, в том числе перевод такой программы или такой базы данных с одного языка на другой язык;
- доведение произведения до всеобщего сведения таким образом, что любое лицо может получить доступ к произведению из любого места и в любое время по собственному выбору (доведение до всеобщего сведения) и ряд иных действий.

При этом, в отличие от иных правомерно обнародованных произведений воспроизведение исключительно в личных целях программ для ЭВМ без согласия автора или иного правообладателя и без выплаты вознаграждения – не допускается.

Согласно положениям ст. 1280 ГК РФ лицо, правомерно владеющее экземпляром программы для ЭВМ или экземпляром базы данных (пользователь), вправе без разрешения автора или иного правообладателя и без выплаты дополнительного вознаграждения:

- внести в программу для ЭВМ или базу данных изменения исключительно в целях их функционирования на технических средствах пользователя и осуществлять действия, необходимые для функционирования таких программы или базы данных в соответствии с их назначением, в том числе запись и хранение в памяти ЭВМ (одной ЭВМ или одного пользователя сети), а также осуществить исправление явных ошибок, если иное не предусмотрено договором с правообладателем;
- изготовить копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей или для замены правомерно приобретенного экземпляра в случаях, когда такой экземпляр утерян, уничтожен или стал непригоден для использования. При этом копия программы для ЭВМ или базы данных не может быть использована в иных целях, чем цели, указанные в подпункте 1 настоящего пункта, и должна быть уничтожена, если владение экземпляром таких программы или базы данных перестало быть правомерным.
- изучать, исследовать или испытывать функционирование программы для ЭВМ в целях определения идей и принципов, лежащих в основе любого элемента программы для ЭВМ, путем осуществления вышеуказанных действий;
- воспроизвести и преобразовать объектный код в исходный текст (декомпилировать программу для ЭВМ) или поручить иным лицам осуществить эти действия, если они необходимы для достижения способности к взаимодействию независимо разработанной этим лицом программы для ЭВМ с другими программами, которые могут взаимодействовать с декомпилируемой программой, при соблюдении следующих условий:

- информация, необходимая для достижения способности к взаимодействию, ранее не была доступна этому лицу из других источников;
- указанные действия осуществляются в отношении только тех частей декомпилируемой программы для ЭВМ, которые необходимы для достижения способности к взаимодействию;
- информация, полученная в результате декомпилирования, может использоваться лишь для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, не может передаваться иным лицам, за исключением случаев, когда это необходимо для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ, или для осуществления другого действия, нарушающего исключительное право на программу для ЭВМ.

Заключение лицензионных договоров о предоставлении права использования программы для ЭВМ или базы данных допускается путем заключения каждым пользователем с соответствующим правообладателем договора присоединения, условия которого *изложены на приобретаемом экземпляре таких программы или базы данных либо на упаковке этого экземпляра*. Начало использования таких программы или базы данных пользователем, как оно определяется этими условиями, означает его согласие на заключение договора.[164]

При этом ст.1259 ГК РФ, определяя понятие объекта авторских прав, устанавливает их независимость от способа выражения произведения. Таким образом, результат интеллектуальной деятельности можно определить как документированную информацию только в частном случае. При этом результаты не могут отчуждаться или иными способами переходить от одного лица к другому в силу требований закона, что дает возможность производить отчуждение (иной переход права) лишь материальных носителей, в которых выражены соответствующие результаты или средства, либо прав на эти результаты.

[164] ст. 1286 ГК РФ

Взаимосвязь между материальным носителем и права на результаты интеллектуальной деятельности раскрывается путем применения понятия контрафакта, определение которого не представлено в законодательстве, но из содержания ст. 1252 ГК РФ следует, что контрафакт обладает следующей совокупностью признаков[165]:

- материальность носителя;

- выраженность в материальном носителе результата интеллектуальной деятельности или средства индивидуализации;

- нарушение исключительного права на такой результат или на такое средство в случае изготовления, распространения, иного использования, импорта, перевозки или хранения материальных носителей.

Здесь следует не согласиться с мнением Иванова Н.В., определяющего, что контрафакт определяется как собирательное понятие, включающее две категории объектов[166]:

- вещи, содержащие результаты интеллектуальной деятельности или приравненные к ним объекты, которые были изготовлены или использованы при отсутствии необходимого разрешения исключительного права на соответствующие объекты, что установлено вступившим в законную силу актом компетентного органа правоприменения;

- вещи, основным предназначением которых является изготовление или иное использование материальных носителей, содержащих результаты интеллектуальной деятельности или приравненные к ним объекты при отсутствии разрешения обладателя исключительного права, что установлено вступившем в законную силу актом компетентного органа правоприменения.

Гражданско-правовая ответственность за использование результата интеллектуальной деятельности или средства индивидуализации без согласия правообладателя определяется ст.ст. 1253, 1301,1311, 1472, 1515, 1537 ГК РФ.

Правовыми последствиями являются:

- материальные носители считаются контрафактными;

---

[165] Елин В.М. Значение гражданско-правовых механизмов защиты компьютерной информации в условиях информационного общества // Проблемы информационной безопасности. Компьютерные системы. 2015. №1. С. 74-82

[166] Интеллектуальная собственность. Контрафакт. Актуальные проблемы теории и практики: сб.науч.трудов. т. 2 /под ред. В.Н.Лопатина. М., 2009. С. 48

- материальные носители по решению суда подлежат изъятию из оборота и уничтожению без какой бы то ни было компенсации;

- оборудование, прочие устройства и материалы, главным образом используемые или предназначенные для совершения нарушения исключительных прав на результаты интеллектуальной деятельности и на средства индивидуализации, по решению суда подлежат изъятию из оборота и уничтожению за счет нарушителя;

- возмещение убытков или выплата компенсации;

- иные последствия предусмотренные законодательством.

Вопрос о допустимости принудительного изъятия из оборота и уничтожения имущества достаточно подробно рассмотрен рядом российских исследователей[167].

Формулировка о том, что материальный носитель «считается» контрафактным представляется достаточно спорной, поскольку термин «считать» в переносном смысле определяется как «принимать во внимание, признавать имеющим значение»[168]. При этом совершенно неопределенным является субъектный состав лиц, правовые последствия, основание и ряд иных юридически значимых обстоятельств, при которых носитель «считается контрафактным».

Несмотря на то обстоятельство, что понятие контрафакта до настоящего времени в полном объеме не раскрывается, при этом «отсутствует единая, понятная и прозрачная методика определения уровня контрафактности на основе объективных показателей как на национальном, так и на международном уровнях. Поэтому, к различного рода рейтингам и коэффициентам, показателям, публикуемым в этой области, следует относиться с достаточной степенью допуска и условности»[169].при этом

[167] Лопатин В.Н. Контрафакт как правовой институт защиты интеллектуальной собственности и обеспечения экономической безопасности; Гаев А.В,.,. Федоров В.А. Юридическая ответственность за правонарушения в сфере интеллектуальной собственности в России /[167] Интеллектуальная собственность. Контрафакт. Актуальные проблемы теории и практики: сб.науч.трудов. т. 2 /под ред. В.Н.Лопатина. М., 2009 С. 36, 124

[168] Большой современный словарь русского языка в 3-х томах. Ефремова Т.Ф. М., 2006.

[169] Лопатин В.Н. Государство и интеллектуальная собственность: переход к инновационной экономике // Интеллектуальная собственность. Актуальные проблемы теории и практики: Сборник научных трудов. Т. 1 / Под ред. В.Н. Лопатина. Юрайт, 2008. С. 17 - 50.

имеется значительное количество судебных решений о выплате компенсаций за незаконное использование результатов интеллектуальной деятельности[170]. Руководящие разъяснения Пленумов верховного суда также не добавляют ясности в этот вопрос. Постановление Пленума Верховного суда[171] № 15 оперирует понятие «является» и им определено, что «контрафактными являются экземпляры произведения и фонограммы, изготовление и распространение которых влечет за собой нарушение авторских и смежных прав. Например, правомерно воспроизведенные и распространяемые на территории другой страны экземпляры произведений, не предназначенные для распространения на территории Российской Федерации, являются контрафактными при распространении на территории Российской Федерации.

Нарушение существенных условий авторского договора является нарушением авторского права, так как указанные действия осуществляются за пределами правомочий, предоставленных автором.

Экземпляры произведений и фонограмм, изготовленные и (или) распространенные с нарушением существенных условий договора о передаче исключительных прав, являются контрафактными. В частности, если воспроизведение превышает тираж, предусмотренный в договоре, то превышение тиража следует рассматривать как нарушение авторского права и смежных прав.

Контрафактными являются и экземпляры произведений и объектов смежных прав, в которых наряду с правомерно используемыми объектами авторского права и смежных прав используются неправомерно воспроизведенные (например, глава в книге, рассказ или статья в сборнике либо фонограмма на любом материальном носителе).

Лицо, осуществившее подобное воспроизведение, может за свой счет удалить контрафактные элементы из экземпляров произведения и (или) объектов смежных прав. В таком случае экземпляры произведений и (или)

---

[170] Постановление Президиума ВАС РФ от 26.06.2012 № 2384/12 по делу № А40-146649/10-19-1260; Определение ВАС РФ от 27.03.2013 № ВАС-3545/13 по делу № А40-134373/11-19-265; Определение ВАС РФ от 21.03.2013 № ВАС-3540/13 по делу № А40-23850/12-27-216; Определение ВАС РФ от 08.02.2013 № ВАС-4/13 по делу № А40-95878/11-26-717; Постановление Президиума ВАС РФ от 27.11.2012 № 9414/12 по делу № А13-8185/2011

[171] П. 16 Постановления Пленума Верховного Суда РФ от 19.06.2006 № 15 «О вопросах, возникших у судов при рассмотрении гражданских дел, связанных с применением законодательства об авторском праве и смежных правах» // БВС РФ № 8, август, 2006

объектов смежных прав не будут считаться контрафактными. Однако это не освобождает нарушителя от гражданско-правовой ответственности…»

Толкование п. 25 Постановления Пленума Верховного Суда РФ N 5, Пленума ВАС РФ N 29 от 26.03.2009 повторяет содержание п. 4 ст. 1252 ГК РФ, однако уточняет, что материальный носитель может быть признан контрафактным только судом[172].

Постановление Пленума Верховного Суда РФ от 26.04.2007 N 14 в п. 5 определяет, что экземпляры произведений или фонограмм считаются контрафактными, если изготовление, распространение или иное их использование, а равно импорт таких экземпляров нарушает авторские и смежные права, охраняемые в соответствии с законодательством Российской Федерации[173].

Таким образом, возникает смешивание понятий: «считаются», «являются», «признаются».

При этом понятие контрафакта применяемое в гражданском законодательстве, нашло свое отражение в ст. 7. 12 Кодекса Российской Федерации об административных правонарушениях, предусматривающей административную ответственность за ввоз, продажу, сдачу в прокат или иное незаконное использование экземпляров произведений или фонограмм в целях извлечения дохода в случаях, если экземпляры произведений или фонограмм являются контрафактными в соответствии с законодательством Российской Федерации об авторском праве и смежных правах либо на экземплярах произведений или фонограмм указана ложная информация об их изготовителях, о местах их производства, а также об обладателях авторских и смежных прав, а равно иное нарушение авторских и смежных прав в целях извлечения дохода.

Ст. 146 УК РФ в ч. 2 предусматривает уголовную ответственность за равно приобретение, хранение, перевозку контрафактных экземпляров произведений или фонограмм в целях сбыта.

---

[172] Постановление Пленума Верховного Суда РФ № 5, Пленума ВАС РФ № 29 от 26.03.2009 «О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации» // БВС РФ № 6, июнь, 2009

[173] Постановление Пленума Верховного Суда РФ от 26.04.2007 № 14 «О практике рассмотрения судами уголовных дел о нарушении авторских, смежных, изобретательских и патентных прав, а также о незаконном использовании товарного знака» // БВС РФ № 7, июль, 2007

Характеризуя тенденции в борьбе с контрафактом, обращает на себя внимание не только неопределенность понятия «контрафакт», но также осознанная жесткость мер в данной сфере. При этом в обществе преобладают настроения, признающие необходимость выплаты вознаграждения правообладателям результатов, однако при этом не существует ни моральных, ни традиционных запретов на неправомерное использование результатов чужой интеллектуальной деятельности. Дополнительно следует иметь в виду, что существующие технологии предельно упростили процесс воспроизведения произведения, под которым понимается изготовление одного и более экземпляра произведения или его части в любой материальной форме. При этом встает вопрос о последовательности борьбы с пиратством, значимости данной деятельности в современном обществе, окончательных целях и задачах этой борьбы.

Обращаясь к зарубежному опыту легко увидеть тенденции гражданско-правовой защиты результатов интеллектуальной деятельности в условиях применения информационных технологий. Так, проект закона Stop Online Piracy Act (SOPA- Закон о пиратстве в интернете), внесен 26 октября 2011 года в качестве билля, который не был принят, однако достаточно четко определил направления деятельности[174], которые могут быть использованы для выработки стратегических аспектов борьбы с нарушениями в данной сфере:

Деятельность Генеральной прокуратуры США в указанной сфере направлена на защиту американских интернет - клиентов и предотвращение поддержки сервис-провайдерами США иностранных вредоносных (infringing) сайтов. Такие сайты подлежат аресту. Генеральный прокурор США может принимать меры в отношении регистратора доменного имени, владельца или оператора указанного иностранного сайта. По постановлению суда могут приниматься меры различного характера к сервис-провайдерам, провайдерам платных сетей, к технологическим процедурам интернет-поиска, к услугам интернет-рекламы в части предоставления услуг пользователям либо исполнения обязательств.

Ст. 103 SOPA раскрывает рыночные механизмы защиты американских пользователей и прекращение финансирования сайтов, направленных на

174 Жарова А.К., Елин В.М. Правовая Характеристика законопроекта США «О пиратстве в интернете» или Online Piracy Act (SOPA) // СПС «Гарант» / Электронный ресурс/ Актуальные статьи

хищение собственности США. При этом хищения, направленные на собственность США определяются как интернет-сайт или часть американо-направленного сайта, используемого пользователями США и ориентированного в первую очередь на нарушение авторских прав, обход системы защиты авторских прав, торговлю поддельными товарами или услугами, либо оператор, который совершает вышеуказанные действия.

Для реализации положений статьи каждый сервис-провайдер и др. информационные субъекты, ведущие деятельность в сети интернет, обязаны предоставить сведения о себе и другую контактную информацию, которая вносится в надлежащий реестр. Статьей определяется порядок разрешения гражданско-правового спора в судебном порядке, а также действия по постановлению суда.

Статья 107 определяет прямой запрет на использование денежных средств США в деятельности иностранных нарушителей (Denying u.s. Capital to notorious foreign infringers). Она содержит критерии, по которым можно определить иностранных нарушителей, чья деятельность наносит значительный ущерб владельцам прав интеллектуальной собственности в США. Правообладатели наделяются правами обращения с запросом к кредитным организациям США о блокировании платежей от клиентов сайтов, нарушающих их права. Если кредитные организации не выполнят требование правообладателей, то последний имеет право обратиться в суд, с иском о блокировании сайтов в получении рекламы и различных платежей из США. Полномочия в данной сфере переданы Координатору органа интеллектуальной собственности, в полномочия которого входит анализ следующей информации:

- анализ иностранных нарушителей с указанием того, как эти нарушители нарушают отраслевые нормы, касающиеся защиты интеллектуальной собственности;
- анализ размеров вреда, причиненного иностранными нарушителями потребителям, бизнесу и интеллектуальной собственности в промышленности США и за рубежом;
- отчет о том, намеревались или преуспели иностранные нарушители в получении доступа к рынкам и капиталу США для финансирования или публичного размещения акций;

- оценку возможности судебного преследования иностранных нарушителей по законодательству их страны;
- обсуждение конкретных рекомендаций в отношении политики по сдерживанию деятельности иностранных нарушителей, включая информацию о том, необходим ли законодательный запрет на попытки привлечения капитала указанных нарушителей в США, включая размещение акций для продажи населению, и будет ли правительство Соединенных Штатов инициировать процесс выявления и составления списка иностранных нарушителей.

2.3. Значение ноу-хау и режима коммерческой тайны в практической деятельности обеспечения информационной безопасности

В условиях, когда информация фактически является товаром, а правовых механизмов осуществления сделок в отношении информации не предусмотрено, начинается поиск вариантов осуществления юридического сопровождения реальных сделок по предоставлению коммерчески значимой информации. При этом наибольший интерес представляет возможность использования режима коммерческой тайны в хозяйственной деятельности. Возможность такого использования строится на том, что секрет производства (ноу-хау) составляют сведения, представляющие коммерческую ценность, в отношении которых введен режим коммерческой тайны. Поскольку ноу-хау относится к результатам интеллектуальной деятельности, постольку правообладатель имеет возможность распоряжаться исключительными правами на такие результаты, но не самими результатами и не содержащимися в них информацией.
При этом, законодатель информацию как инстумент оптимзации процессов, экономии средств и полноценного товарана рынке. Существует мнение, что в будущем непрерывное развитие технологий будет сопровождается перечнем различных процессов, которые постепенно можно улучшать, оптимизировать, добавлять и т.п. с целью эффективного и экономичного достижения результата[175].

[175] См.: *Ситишко Д.А.* Секрет производства (ноу-хау) и коммерческая тайна: некоторые особенности использования секрета производства // Право и политика, 2009, № 4

Несмотря на то обстоятельство, что российском законодательстве исследователями насчитывается около 40 видов тайн[176], особое внимание как законодателя, так и хозяйствующего субъекта привлекает вопрос ответственности юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях информации, содержащей коммерческую тайну[177]. Недаром определено, что составной частью инсайдерской информации выступают сведения, составляющие коммерческую тайну[178], распространение которых может оказать существенное влияние на цены финансовых инструментов, иностранной валюты и (или) товаров одной или нескольких управляющих компаний инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов…

С практической точки зрения использование коммерческой тайны находит свое отображение в нормах Трудового кодекса Российской Федерации[179],определяющих, что в качестве дополнительного условия трудового договора между работником и работодателем может указываться запрет на разглашение охраняемой законом государственной, служебной, коммерческой и иной тайны (ст.57 ТК РФ). Расторжение трудового договора по инициативе работодателя может осуществляться в случае разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей (ст. 81 ТК РФ). При этом разглашение сведений, составляющих охраняемую законом тайну (государственную, служебную, коммерческую или иную) представляет собой основание применения полной материальной ответственности к работнику (п.7 ст.243 ТК РФ).

---

[176] Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник / Под ред. акад. РАН Б.Н. Топорнина.. СПб., 2005.

[177] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // РГ, № 187, 28.09.2000 г.

[178] Федеральный закон от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ от 2 августа 2010 г. № 31 ст. 4193

[179] Трудовой кодекс Российской Федерации // СЗ РФ, 07.01.2002, № 1 (ч. 1), ст. 3.

Следует иметь в виду, что нарушение требований законодательства о коммерческой тайне влечет за собой не только дисциплинарную, но также и уголовную ответственность, поскольку в нормах ст. 183 УК РФ предусматривается уголовная ответственность за собирание сведений, составляющих коммерческую тайну путем похищения документов, подкупа или угроз, а равно иным незаконным способом, а также за незаконные разглашение или использование сведений, составляющих коммерческую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе.

Перечнем сведений конфиденциального характера[180] коммерческая тайна определяется как сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами. Правовой статус коммерческой тайны определяется Федеральным законом от 29.07.2004 N 98-ФЗ «О коммерческой тайне»[181].

При наличии научного спора об общих чертах и различии коммерческой тайны и секрета производства[182], правовое регулирование обращения информации, составляющей коммерческую тайну, осуществляется исходя из дуалистического подхода – нормами Федерального Закона «О коммерческой тайне» и положениями Гл. 75 части четвертой Гражданского кодекса Российской Федерации[183].

Информацией, составляющей коммерческую тайну, могут выступать сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности[184].

Критерием отнесения информации к коммерческой тайне выступает действительная или потенциальная коммерческая ценность информации в силу неизвестности третьим лицам, к которой у третьих лиц нет свободного

---

[180] Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» // СЗ РФ, № 10, ст. 1127,

[181] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СЗ РФ, № 32, ст. 3283

[182] Потрашкова О.А. Права на секреты производства (ноу-хау) // Интеллектуальная собственность. Актуальные проблемы теории и практики: Сборник научных трудов. Т. 1 / Под ред. В.Н. Лопатина. Издательство "Юрайт", 2008

[183] Ч. 4 ГК РФ регламентирует правоотношения в сфере права интеллектуальной собственности (права на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации).

[184] Ст. 3 ФЗ РФ «О коммерческой тайне»

доступа на законном основании и в отношении которой обладателем таких сведений введен режим коммерческой тайны.

Особенностью коммерческой тайны является определенная близость ее правового режима к правовому режиму тайны государственной, поскольку Законами «О государственной тайне» и «О коммерческой тайне» максимально раскрыт комплекс мероприятий, направленных на обеспечение защиты сведений, и регламентирован следующий круг вопросов:

- определен перечень сведений, составляющих, а главное, не могущих составлять государственную и коммерческую тайну;
- определен круг органов, осуществляющих защиту государственной и коммерческой тайны и пределы их полномочий;
- установлен порядок отнесения сведений к государственной и коммерческой тайне, порядок засекречивания и рассекречивания сведений и их носителей;
- указаны реквизиты носителей сведений, составляющих данные категории тайны;
- определены порядок допуска лиц к указанным категориям сведений, их права и обязанности;
- установлен порядок предоставления сведений, составляющих государственную и коммерческую тайну.

При этом, в отличие от тайны государственной, возможность отнесения информации к сведениям, составляющим коммерческую тайну, в полной мере относится к ведению обладателя указанной информации. При этом установление режима коммерческой тайны невозможно по ряду категорий сведений, определяемых ст. 5 ФЗ «О коммерческой тайне»:

- содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
- содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
- о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

- о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;
- о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;
- о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;
- о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;
- об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
- о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;
- о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
- обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

В том, что касается иной информации, режим коммерческой тайны считается установленным после принятия следующего комплекса мер, предусмотренного ст. 10 ФЗ РФ «О коммерческой тайне».

При этом решение о введении режима коммерческой тайны принимается исполнительным органом организации по единственному формальному основанию получения возможности «…при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, … или получить иную коммерческую выгоду»[185].

[185] Ст. 1 ФЗ «О коммерческой тайне»

Содержание режима коммерческой тайны включает в себя пять обязательных шагов:

- определение перечня информации, составляющей коммерческую тайну;
- ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
- регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Наряду с указанными мерами, обладатель информации вправе применять при необходимости средства и методы технической защиты и другие меры не противоречащие законодательству. Указанные меры принято делить на тесно взаимосвязаны между собой[186] правовые, организационные и технические. Более того, большинство превентивных мер изначально включают в себя и правовую, и организационную, и техническую составляющие.

Организационные меры включают в себя: работу с сотрудниками, контроль режима защиты документов, определение формы и содержания документов, классификацию документов и простановку грифа. К мерам технического характера можно отнести установку сигнализации и контроль за ее работой, использование специальных замков и других устройств, использование устройств для уничтожения документов, обеспечение сотрудников сейфами и специальными контейнерами для хранения документов. Специальные меры включают: применение средств защиты от копирования документов,

[186] Погуляев В.В. Постатейный комментарий к Федеральному закону «О коммерческой тайне»

применение устройств скрытого фиксирования незаконного доступа к документам, защиту от промышленного шпионажа, проведение служебного расследования при утрате документов.

Согласно положениям ст. 10 ФЗ «О коммерческой тайне» меры по охране конфиденциальности информации признаются разумно достаточными, если исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя; а также обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

Дисциплинарная ответственность работника возникает только после выполнения участниками трудового отношения комплекса правовых мер, направленных на осуществление правового режима охраны конфиденциальности сведений, составляющих коммерческую тайну, в рамках трудовых отношений. Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями, причем работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением им трудовых обязанностей.

В целях охраны конфиденциальности информации работодатель обязан: ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты; с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение; а также создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

В целях охраны конфиденциальности информации работник обязан: выполнять установленный работодателем режим коммерческой тайны; не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях; передать работодателю при

прекращении или расторжении трудового договора имеющиеся в пользовании работника материальные носители информации, содержащие информацию, составляющую коммерческую тайну

Согласно ст. 1465 ГК РФ секрет производства (ноу-хау) составляют сведения, относящиеся к информации, составляющей коммерческую тайну, в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Секрет производства, отвечая всем признакам, свойственным интеллектуальной собственности, обладает рядом специфических особенностей. Прежде всего, в основе секрета производства лежит фактическая монополия определенного лица на некоторую совокупность знаний, хотя частью четвертой ГК РФ за обладателями секретов производства признается и юридическая монополия на их использование — исключительное право.

При этом можно назвать следующие отличия секретов производства (ноу-хау) от иных объектов интеллектуальной собственности:

- ноу-хау обладает наибольшей универсальностью. Так, если под изобретениями, промышленными образцами, товарными знаками и иными объектами интеллектуальной собственности закон понимает вполне определенные результаты, то под понятие секрета производства могут быть подведены самые разнообразные сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предпринимателя. Несмотря на это, к секрету производства могут быть отнесены и патентоспособные решения. Эту особенность используют заявители в случае подачи заявки на выдачу патента в федеральный орган исполнительной власти. Заявители на срок прохождения регистрации вводят режим коммерческой тайны для своих объектов;
- в законодательном порядке закреплены различные требования, которым должны соответствовать сведения для предоставления им правовой охраны в качестве объектов интеллектуальной собственности и в качестве секретов производства;
- патентная охрана, и охрана секретов производства предоставляется только тем сведениям, которые отвечают критериям охраноспособности, закрепленным в нормах ГК РФ. В свою очередь факт соответствия сведений

условиям охраноспособности устанавливается по-разному в зависимости от вида предоставляемой охраны;

- исключительное право на изобретение, полезную модель и промышленный образец возникает в результате регистрационных действий, осуществляемых государством в лице федерального органа исполнительной власти по интеллектуальной собственности;

- в отношении секрета производства действует неограниченный срок его охраны. Право на секрет производства действует до тех пор, пока сохраняется фактическая монополия лица на информацию, которая его образует, а также имеются предусмотренные законом условия его охраны. то обстоятельство делает избрание данной формы охраны привлекательным для предпринимателей в тех случаях, когда их не удовлетворяет принцип срочности патентной охраны;

- проверка охраноспособности секрета производства осуществляется не в порядке специальной предварительной процедуры, а только тогда, когда право на секрет производства нарушается или оспаривается и требуется установить, существует ли оно вообще.

В соответствии со ст. 1229 ГК РФ обладателю секрета производства принадлежит исключительное право использовать его любым не противоречащим закону способом, в том числе при изготовлении изделий и реализации экономических и организационных решений.

Закон предопределяет, что обладатель секрета производства может распоряжаться исключительным правом на секрет производства, т.е. допускается отчуждение или выдача третьим лицам лицензий, которые в свою очередь могут носить исключительный или неисключительный характер. Предметом таких лицензий выступает коммерчески-значимая информация: т.е., чаще всего, технологические секреты, опыт управленческой, финансовой и производственной деятельности и т.п., которые не имеют патентной охраны, но представляют большую коммерческую ценность.

Для осуществления указанной деятельности в отношении секрета производства надлежит осуществить комплекс мероприятий по постановке его на бухгалтерский учет, регламентация которых осуществляется на

основании Положения по бухгалтерскому учету «Учет нематериальных активов»[187].

Постановка на учет исключительных имущественных прав на секреты производства в качестве нематериальных активов предполагает составление акта произвольной формы, в котором должны быть отражены следующие сведения:

- наименование документирующего акта;
- дата составления документирующего акта;
- наименование субъекта предпринимательской деятельности, составившего документирующий акт;
- указание на основание, позволяющее использовать исключительные имущественные права (первоначальные, производные способы возникновения права собственности на объект);
- экономические показатели хозяйственной операции с объектом интеллектуальной промышленной собственности в натуральном и денежном выражении;
- указание должностных лиц, ответственных за введение в хозяйственный оборот исключительных имущественных прав на объекты интеллектуальной промышленной собственности;
- подписи должностных лиц, ответственных за введение в хозяйственный оборот изобретений, полезных моделей, промышленных образцов, ноу-хау[188].

После составления документирующего акта на исключительные имущественные права по поводу использования объектов интеллектуальной промышленной собственности оформляется Карточка учета нематериальных активов (форма НМА-1), утвержденная Постановлением Госкомстата 30 октября 1997 г. N 71а[189].

Положением также определяется порядок последующей оценки нематериальных активов, их амортизация, списание и ряд иных вопросов.

---

[187] Приказ Минфина РФ от 27.12.2007№ 153н «Об утверждении Положения по бухгалтерскому учету «Учет нематериальных активов» (ПБУ 14/2007)» с изм. Приказом Минфина РФ от 25 октября 2010 № 132н // РГ, № 22, 02.02.2008

[188] Сенников Н.Л. Документирование объектов интеллектуальной промышленной собственности // Налоги, 2006, № 2

[189] Постановление Госкомстата РФ от 30.10.1997 № 71а (ред. от 21.01.2003) «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты, основных средств и нематериальных активов, материалов, малоценных и быстроизнашивающихся предметов, работ в капитальном строительстве» // «Нормативные акты по финансам, налогам, страхованию и бухгалтерскому учету», № 1, 1998

Согласно действующему законодательству[190], направленному на совершенствование отношений в указанной сфере, от налогообложения освобождены операции, связанные с передачей исключительных прав на секреты производства (ноу-хау) на основании лицензионных договоров, поскольку это эффективно способствует развитию секрета производства как объекта товарного рынка.

При определении реальной стоимости прав на результаты интеллектуальной деятельности следует иметь в виду четыре основных направления теории права интеллектуальной собственности США, занимающих основные позиции в сфере практического использования результатов интеллектуальной деятельности[191]:

- -утилитарная теория;
- трудовая теория;
- персональная теория;
- теория социального планирования.

В основе утилитарной теории лежит концепция приведения к максимуму чистого общественного достояния, поскольку имущественные права стимулируют создание произведений литературы, науки и искусства и изобретений, а также сокращают возможность пользоваться полученными результатами[192]. Основная задача авторского права состоит в создании механизма возмещения затрат на создание произведения и получение автором дохода. При этом в условиях рыночной экономики следует обеспечить автору доступ к созданному продукту и за счет этого самостоятельно устанавливать размер оплаты.

Трудовая теория основывается на том, что система права интеллектуальной собственности связана с естественным правом, поскольку каждый, кто приложил труд к ресурсам, не имеющим собственника, имеет право полной власти над результатом труда[193].

---

[190] Федеральный закон от 19.07.2007 № 195-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части формирования благоприятных налоговых условий для финансирования инновационной деятельности» // СЗ РФ. № 31. Ст. 3991

[191] Бабин С.А. Интеллектуальная собственность в сети «Интернет». М., 2005. С. 90

[192] William Landes, Richard Posner “An economic Analysis of copyright Law” // Journal of legal Studies.1989. # 18; William Landes, Richard Posner “Trademark Law: An economic Perspective” //Journal of Law and Economics. 1987. # 30

[193] Justin Hughes. The Philosophy of intellectual property // Georgetown Law Journal. 1988. # 77

Персональная теория основывается на постулате о том, что продукт интеллектуальной деятельности, будучи продолжением личности его создателя, должна охраняться именно в этом качестве, способствовать процветанию людей, защищая и поддерживая фундаментальные человеческие нужды и интересы.

Теория социального планирования несколько расширяет утилитарную[194] и рассматривает не только экономический эффект, но также духовную, культурную и политическую сферу общественной жизни.

Однако указанные теории совершенно не объясняют пристальное внимание к построению реально действующей системы обеспечения защиты прав авторов и правообладателей.

Рассматривая вопрос о защите результатов интеллектуальной деятельности с точки зрения концепции международного разделения труда, обращает на себя внимание то обстоятельство, что в целом специфика производства результатов интеллектуальной деятельности заключается в получении значительных доходов при сравнительно незначительных затратах. Конечно, размеры этих затрат можно увеличивать искусственно (как в шоу-бизнесе), либо естественным путем (стартап-проекты на всех этапах развития: от разработки идеи до её коммерциализации). В любом случае экономический эффект данной деятельности колоссальный. «В стоимости так называемой лицензионной продукции в западных компаниях оплата авторского труда и труда тех, кто произвел эту продукцию составляет 5-6 % стоимости товара, а 90 % и более – это сверхприбыль, которую никак нельзя причислить к вознаграждению авторского труда»[195].

Определяя затраты, связанные с производством результатов интеллектуальной деятельности фактическую стоимость можно определить исходя из размера оплаты при приобретении или создании актива, что может включать в себя:

- суммы, уплачиваемые в соответствии с договором об отчуждении исключительного права на результат интеллектуальной деятельности или на средство индивидуализации правообладателю (продавцу);

- таможенные пошлины и таможенные сборы;

---

[194] Rosemary J. Coomble. Objects of Property and subjects of Politics^ Intellectual Property Laws and Democratic Dialogue // Texas Law Review. 1991. # 60

[195] Лопатин В.Н. Там же. С. 42

- невозмещаемые суммы налогов, государственные, патентные и иные пошлины, уплачиваемые в связи с приобретением нематериального актива;

- вознаграждения, уплачиваемые посреднической организации и иным лицам, через которые приобретен нематериальный актив;

- суммы, уплачиваемые за информационные и консультационные услуги, связанные с приобретением нематериального актива;

- иные расходы, непосредственно связанные с приобретением нематериального актива и обеспечением условий для использования актива в запланированных целях[196].

Далее на реальную стоимость результатов интеллектуальной деятельности влияют их размеры вознаграждения при их использовании или отчуждении, т.е. потребность общества в этих результатах.

При этом следует учитывать факторы становления и развития международного разделения труда, такие как научно-технический прогресс, различия в уровнях экономического и научно-технического развития стран, наличие подготовленных специалистов, востребованность общества в конкретных результатах конкретных производителей и т.д. Деятельность стран «золотого миллиарда» сосредоточена именно в отраслях, связанных с использованием результатов интеллектуальной деятельности, а реальное производство «выносится» в страны третьего мира. Смещение реального производства происходит туда, где дешевле сырье и рабочая сила. Обращает на себя внимание сохранение при этом прав на средства индивидуализации, к которым относятся: фирменные наименования, товарные знаки и знаки обслуживания, наименования мест происхождения товаров, а также коммерческие обозначения.

По всей видимости, в странах с реально сбалансированными секторами экономики, ситуация по поводу использования в промышленности результатов интеллектуальной деятельности кардинально меняется, поскольку бизнес в некоторой мере заинтересован в использовании более продвинутых технологий, в связи с чем и появляется общественная заинтересованность в разработке результатов интеллектуальной деятельности более высоких уровней. Автор результата интеллектуальной деятельности, осознающий реальную стоимость как своего труда, так и его

[196] Приказ Минфина РФ от 27.12.2007 N 153н «Об утверждении Положения по бухгалтерскому учету "Учет нематериальных активов" (ПБУ 14/2007)» // РГ № 22, 02.02.2008.

результата, не обеспокоен проблемой практического внедрения своего продукта, имея возможность отчуждения или передачи прав, а также имея реальную возможность получения дополнительной выгоды от эксплуатации результата интеллектуальной деятельности. Доходит до того, что крупными исследовательскими концернами (такими как Darpa) к разработке принимаются и оплачиваются не готовые результаты интеллектуальной деятельности, а идеи, концепции, принципы, методы, процессы, системы, способы, решения задач[197], т.е. то, что ни при каких условиях не может быть отнесено к защищаемым результатам интеллектуальной деятельности.

При этом за последние 25 лет в нашей стране катастрофически снизилось количество изобретений, полезных моделей и промышленных образцов. В середине 70-х годов доля России в общем объеме поданных в мире национальных заявок на изобретения составляла 25,8% (для сравнения - США - 14,6%, Японии - 30,6%), а в общем объеме выданных на имя национальных заявителей охранных документов - 22,8% (США -15,1%, Японии - 19,3%); к началу 90-х годов - соответственно 16,2% (США - 12,8%, Японии -46,8%) и 33,4% (США - 19%, Японии - 22,2%), а уже к концу 90-х годов - соответственно 2,6% (США - 15,2%, Японии - 44,6%) и 2,9% (США - 23,4%, Японии - 24,1%)[198]. По всей видимости, катастрофическое падение связано с процессом смены приоритетов.

Руководством страны уделяется большое внимание проблемам внедрения инноваций в экономику. В настоящее время у нас действует более ста федеральных целевых программ[199], так или иначе направленных на придание экономики нашей страны инновационного пути развития. При этом практической реализации не наблюдается ни по формальным отчетам, ни по реальному положению вещей.

В таких условиях реальные рыночные механизмы получения доходов в результате приобретения или использования исключительных прав на результаты интеллектуальной деятельности подменен механизмом получения компенсаций за незаконное использование результатов интеллектуальной деятельности.

---

[197] http://www.darpa.mil/Our_Work/TTO/About.aspx

[198] http://kausarpatent.ru/index.php/izobretatelstvo-v-russia

[199] По данным СПС «Консультант плюс»

2.4. Система уголовно-правового обеспечения информационной безопасности

Законом «Об информации»[200] в качестве ответственности за правонарушения в сфере информации, информационных технологий и защиты информации предусмотрено привлечение к дисциплинарной, гражданско-правовой, административной либо уголовной ответственности в соответствии с законодательством Российской Федерации.

При этом уголовная ответственность представляется самой серьезной, поскольку уголовное законодательство определяет способ выражения государственной воли, возведенной высшим органом законодательной власти в систему юридических норм, предусматривающих основание, принципы и другие общие положения уголовной ответственности, виды преступлений, а также наказания и иные меры уголовно-правового характера за совершение преступлений[201].

С точки зрения международного права под информационной преступностью следует понимать использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях[202].

Значительное число российских авторов определяют информационную преступность как преступные деяния в информационной сфере, где информационная связь выступает по отношению к преступности как ее существенный детерминистский признак[203]. Это связано с тем, что предметом информационных отношений выступает совокупность реально существующих материализованных результатов творчества и труда,

---

[200] Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // СЗ РФ, 31.07.2006, № 31 (1 ч.), ст. 3448

[201] См.: Уголовное право. Учебник Под общ. Ред. Л. Д. Гаухмана, Л.М. Колодкина, С.В. Максимова, М., 1999

[202] Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Заключено в г. Екатеринбурге 16.06.2009) // Бюллетень международных договоров. 2012. № 1. С. 13 - 21.

[203] Горшенков Г.Н. К понятию "информационная преступность" // Российский криминологический взгляд. 2005. № 4. С. 93 - 96; Крылов В.В. Информационные компьютерные преступления. М., 1997. С. 11; Крылов В.В. Информация как элемент криминальной деятельности // Вестник Московского ун-та. Сер. 11. Право. 1998. № 4. С. 55; Рассолов М.М. Информационное право. М., 1999. С. 66.

воплощенных в информации, информационных технологиях и средствах и технологиях коммуникации информации по сетям связи[204]

При этом информация и информационные ресурсы могут рассматриваться, с одной стороны, - как орудия и средства совершения преступления, с другой стороны, как то, на что направлено противоправное деяние.

При анализе информации как орудия, средства и способа совершения преступления[205], следует отметить, что в большинстве случаев (при обсуждении связки "средство - способ") она представлена именно как орудие, средство совершения общественно опасных деяний.

Информация в качестве орудия преступления наиболее выраженно представлена в новелле уголовного законодательства: ст.ст. 159.3, 159.6 УК РФ, предусматривающих уголовную ответственность за совершение мошенничества с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты, а также путем ввода, удаления, блокирования, модификации компьютерной информации.

Как средство, то есть то, с помощью чего совершалось преступление, информация, к примеру, зафиксирована в составах ст. 128-1 «Клевета», ст. 155 «Разглашение тайны усыновления (удочерения)», ст. 185 «Злоупотребление при эмиссии ценных бумаг» и т.д. Особенностью информации как средства совершения преступления является то, что без ее использования будет отсутствовать само преступление. Характеризуя использование информации как средство совершения преступления можно выделить следующие категории противоправных деяний:

- подстрекательство и пособничество;

- **склонение** (ст. 230 УК РФ),
- **принуждение** (ст.ст.179, 302, 309 УК РФ),
- **вовлечение** (ст.ст.150,151,205-1 УК РФ) и
- **понуждение** (ст.133 УК РФ) к осуществлению преступной деятельности;
- **отказ** в предоставлении информации (ст.ст. 287,308 УК РФ), либо **непредставление** информации;

[204] Информационное право: Учебник для ВУЗов /И.Л.Бачило.- М., 2009. С. 25

[205] См.: Яшков С.А Информация и УК РФ: теоретические проблемы применения норм закона // Адвокатская практика, № 4, 2004.

- **осуществление призывов**: к осуществлению террористической деятельности или публичное оправдание терроризма (ст. 205-2 УК РФ), к активному неподчинению законным требованиям представителей власти и к массовым беспорядкам, а равно призывы к насилию над гражданами (ст.212 ч.3 УК РФ), к осуществлению экстремистской деятельности (ст. 280 УК РФ), к развязыванию агрессивной войны (ст.354 УК РФ);
- **возбуждение ненависти либо вражды**, а равно унижение человеческого достоинства (ст. 282 УК РФ);
- **- разглашение и т.д.**

Информация как способ совершения преступления представлена в Уголовном кодексе Российской Федерации только в качестве признаков состава преступления или непосредственно квалифицированного состава. Представляется, что законодателем это сделано потому, что использование информации повышает общественную опасность деяния, а, следовательно, должно отражаться на ответственности за совершение подобного деяния. Например, если клеветнические сведения распространяются в средствах массовой информации, уголовный закон предусматривает за такую клевету повышенную ответственность (ч. 2 ст. 128-1 УК РФ).

Рассматривая информацию как объект преступления, следует иметь в виду, что наряду с господствующей концепцией, согласно которой объектом преступления признаются общественные отношения, в науке уголовного права высказаны и другие точки зрения, что позволяет сформировать три основных подхода: 1) общественные отношения; 2) общественные отношения и производительные силы общества, то есть люди, орудия и средства производства; 3) предмет преступления.

При отнесении информационных правоотношений к родовым или видовым объектам состава преступления, ее компоненты самостоятельно выделяются исключительно в видовой объект главы 28 УК РФ (преступления в сфере компьютерной информации). Прочие охраняемые законом информационные отношения можно отнести к элементам общего объекта состава преступления.

В качестве непосредственного объекта преступления информационные отношения выступают, так или иначе, практически во всех составах преступлений, где информация фигурирует как правовая категория, причем

подсчет указанных составов является занятием малоперспективным и, видимо, бесполезным.

Вопрос о классификации информационных преступлений рассматривался рядом российских ученых и практиков. В основу классификации информационных преступлений, предложенной А.Н.Третьяковым, положена оценка информационных воздействий, произведенных:

- в результате несанкционированного и неправомерного воздействия посторонних лиц на информацию;
- на информационные права и свободы личности;
- в результате воздействия недостоверной, ложной информации, дезинформации на личность, общество и государство[206].

По мнению И.А. Юрченко, следует выделять три группы информационных преступлений:

- посягательства на саму информацию;
- распространение "вредной" (вредоносной) информации;
- посягательства на право граждан и иных субъектов на доступ к открытой информации[207].

Характеризуя информационные преступления, Л.А.Сергиенко выделяет:

- преступления в сфере компьютерной информации;
- правонарушения в сфере неприкосновенности частной жизни;
- нарушения конституционных норм об информационных правах человека;
- преступления в сфере разглашения информации ограниченного доступа;
- похищениями или подделками документов;
- сокрытие значимой информации[208] и др.

По наличию специфичного объекта, как основного, так и дополнительного, способа совершения, предполагающим использование компьютерной сети в качестве средства или орудия преступления, И.Г.Чекунов полагает, что к информационным преступлениям

[206] Третьяков А.Н. Криминологическая характеристика и предупреждение преступности в информационной сфере уголовно-исполнительной системы: Дис.... канд. юрид. наук. Рязань, 2004. С. 166.
[207] Юрченко И.А. Понятие и виды информационных преступлений // Российское право в Интернете. 2003. № 1. URL: http:// www.rpi.msal.ru/ pri№ts/ 200301ugol1.html.
[208] Сергиенко Л.А. История формирования информационного права в СССР и Российской Федерации 1960-2000 гг. Монография.- М., 2013, С. 231-234

представляется возможным отнести по тем или иным основаниям подавляющее число известных современному законодательству преступлений, в связи с чем предлагается следующая классификация[209]:

- преступные деяния, в которых общественные отношения в сфере охраны тех или иных сведений выступают в качестве основного или дополнительного объекта, причем к информационным преступлениям рассматриваемой категории автор относит все преступления, так или иначе связанные с незаконным получением, собиранием и распространением конфиденциальной информации;

- ко второй категории информационных преступлений также может быть причислен большой круг преступных деяний, предусмотренных статьями разных глав УК РФ, что включает в себя преступления против свободы, чести и достоинства личности, конституционных прав и свобод человека и гражданина, против собственности, в сфере экономической деятельности, против общественной безопасности, против здоровья населения и общественной нравственности и против основ конституционного строя и безопасности государства.

Классификация, предлагаемая Букалеровой Л.А. и Пикуровым Н.И.[210], основывается на том, что в 13 нормах предусмотрены незаконные деяния с понятием «информация», по 16 составам Уголовного кодекса предусмотрена ответственность за противоправные деяния со «сведениями», а в 13 нормах охраняются «тайны».

К недостаткам предложенных классификаций можно отнести следующее:

- при использовании в основе классификации понятия «информация» в качестве объекта и предмета преступления, имеет место «размытость» понятия, причем существенной проблемой является само отнесение информации к материальным объектам, поскольку информация у различных авторов может рассматриваться в диапазоне от «…не имеет материальной формы и не зависит от своего материального носителя…

[209] Чекунов И.Г. К вопросу о понятии и системе преступлений, совершаемых с использованием компьютерных сетей // Правовые вопросы связи, 2012, № 1

[210] *Букалерова Л.А., Пикуров Н.И.* Уголовно-правовая охрана оборота официальной информации // Правовые вопросы связи. 2005.№1

поскольку не имеет жестко детерминированной связи с ним»[211], до «…идеальный компонент бытия, не сводимый к тем материальным носителям, на которых она переносится, в связи в чем информация не может рассматриваться как предмет преступления»[212]. При этом, в отношении информации возможны высказывания о том, что она «не только идеальна, но и субъективна, … информация фактически является метафорой для обозначения свойств отображения чего-либо в некоторых данных…»[213].

- ***отсутствие общепринятой практики классификации информации по ряду заявляемых критериев***. Так, в настоящее время существует научная полемика по поводу «открытой» информации, связанная с невозможностью определения вида деятельности по использованию данной информации, а также субъектов, ответственных за размещение. Также существует ряд проблем по поводу составления перечня вредоносной информации, поскольку существует определенная коллизия между законодательно закрепленными перечнями и практическим отнесением информации к данной категории.

- как представленные, так и некоторые иные ***классификации[214] являются искусственными по своей сути***, поскольку, будучи направленными на систематизацию, в качестве основания выбирают признаки, удобные для этой цели, но несущественные для самих предметов.

Исходя из изложенного, классификацию информационных преступлений следует связать с характеристикой информации как объекта правовых отношений. При этом особое внимание обращает на себя информация ограниченного доступа, обязательным условием отнесения к которой, в силу ст. 9 Закона «Об информации», является требование федеральных законов. При этом выстраивается следующая иерархическая картина:

---

[211] Суслопаров А.В. Информационные преступления: Автореф. дис.... канд. юрид. наук. Красноярск, 2008. С. 8, 13 - 14.

[212] Пархоменко В.А. К определению понятия "информационное преступление" // Вестник ИГЭА. 2001. № 2. URL: http://www.etasu.isea.ru/attor№/s5.htm.

[213] Нестеров А.В. Существует ли информационная безопасность, или некоторые аспекты законопроекта технического регламента «О безопасности информационных технологий» // Правовые вопросы связи, 2007, № 1

[214] Доржиев А.В. Уголовно-правовые меры противодействия преступлениям, совершаемым в предпринимательской сфере: Дис.... канд. юрид. наук. М., 2010. С. 154 – 155; Кесареева Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: Автореф. дис.... канд. юрид. наук. М., 2002. С. 6; Крылов В.В. Расследование преступлений в сфере информации. М., 1998. С. 46; Широков В.А., Беспалова Е.В. Киберпреступность: история уголовно-правового противодействия // Информационное право. 2006. № 4. С. 18 - 19; Щепетильников В.Н. Уголовно-правовая охрана электронной информации: Автореф. дис.... канд. юрид. наук. Елец, 2006. С. 13.

- государственная тайна (защита информации осуществляется на основании требований Закона РФ «О государственной тайне»[215]);
- сведения конфиденциального характера перечень определяется положениями Указа Президента РФ № 188[216];
- иная информация ограниченного доступа.

На защиту сведений, составляющих государственную тайну направлен ряд составов преступлений, предусмотренных ст.ст. 275 УК РФ (Государственная измена), 276 УК РФ (Шпионаж), 283 УК РФ (Разглашение государственной тайны), 283.1 УК РФ (Незаконное получение сведений, составляющих государственную тайну), 284 УК РФ (Утрата документов, содержащих государственную тайну).

По поводу защиты данной категории сведений имеется значительное количество открытой научной и практической литературы, Руководящих разъяснений ПВС РФ, судебной практики. Анализ системы позволяет сделать вывод о тщательности проработки данной категории составов преступлений, учитывающих специфику субъекта, субъективной и объективной стороны, обеспечивающих охват преступных деяний при различных условиях совершения преступления.

Президентский Перечень сведений конфиденциального характера, отраженный в Указе № 188, определяет категории информации ограниченного доступа, которые достаточно близки (хотя и не идентичны) категориям сведений, охраняемым уголовным законодательством:
- о частной жизни лица (ст. 137 УК РФ), тайне усыновления (удочерения) (ст.155 УК РФ);
- о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса (ст.311 УК РФ) и о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа (ст.320 УК РФ).
- данные предварительного расследования (ст.310 УК РФ);
- сведения, составляющие коммерческую, налоговую или банковскую тайну (ст.183 УК РФ);

[215] Закон РФ от 21.07.1993 № 5485-1 "О государственной тайне" // СЗ РФ 13.10.1997, № 41, стр. 8220-8235
[216] Указ Президента Российской Федерации № 188 от 06 марта 1997г. «Об утверждении перечня сведений конфиденциального характера» (в ред Указа Президента РФ № 1111 от 12.09.2005г.)

- информация, относящаяся к тайне переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст.138 УК РФ);
- сведений, составляющих сущность результата интеллектуальной деятельности (ст.ст. 146, 147, 180, 183 УК РФ).

При этом следует иметь в виду, что определяя информацию как объект правовых отношений, закон взаимосвязывает информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Запрет на распространение информационных продуктов находит свое отражение в положениях Федеральных законов «О СМИ»[217] и «О защите детей от информации, причиняющей вред их здоровью и развитию»[218] и др. Предусмотрена уголовная ответственность за информационную деятельность в отношении информации, распространение которой запрещено[219].

При анализе уголовного законодательства модно выделить ряд вредоносных информационных объектов:
- информационные объекты, подрывающие основы морали, нравственности и правопорядка в обществе;
- информационные объекты, унижающие человеческое достоинство;
- ложная, фальсифицированная информация;
- информационные объекты, направленные на осуществление противоправного информационного воздействия;
- информационные объекты, способствующие совершению преступлений.

К категории *информационных объектов, подрывающих основы морали, нравственности и правопорядка в обществе* следует относить:
- порнографические материалы (ст.ст. 242, 242-1 УК РФ);
- информацию, вовлекающую в совершение преступления и занятия антиобщественной деятельностью (ст.ст. 150, 151, 205-1, 240 УК РФ);
- информационные объекты, содействующие совершению незаконных сделок или финансовых операций (ст.ст. 170.1, 173.2, 174, 174-1, 176 УК РФ).

К категории информационных *объектов унижающих человеческое достоинство* относится:

[217] Закон РФ от 27.12.1991 N 2124-1 «О средствах массовой информации» // РГ, № 32, 08.02.1992,
[218] Федеральный закон от 29.12.2010 N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ, 03.01.2011, № 1, ст. 48
[219] Ст.5 Закона «Об информации»

- собственно информация, определенная законодателем как «унижающая человеческое достоинство» (ст.ст. 110, 335 УК РФ);
- «аффектирующая» информация (ст.ст. 107,113 УК РФ);
- клеветническая информация (ст. 128.1 УК РФ);
- оскорбительная информация (ст.ст. 297, 319, 336 УК РФ).

Ложную, фальсифицированную информацию можно подразделять на следующие категории:

- распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию (ст. 128.1 УК РФ);
- предоставление гражданину неполной или заведомо ложной информации должностным лицом (ст. 140 УК РФ);
- предоставление заведомо ложной информации при осуществлении экономической деятельности: (ст.ст.176, 185, 185.1, 197, 198, 199 УК РФ);
- заведомо ложное сообщение об акте терроризма (ст.207 УК РФ);
- предоставление заведомо неполной либо ложной информации Совету Федерации Федерального Собрания Российской Федерации, Государственной Думе Федерального Собрания Российской Федерации или Счетной палате Российской Федерации, если эти деяния совершены должностным лицом, обязанным предоставлять такую информацию (ст.287 УК РФ);
- внесение в официальные документы заведомо ложных сведений должностным лицом (служебный подлог) (ст.292 УК РФ);
- в сфере осуществления правосудия: заведомо ложный донос (ст.306 УК РФ), заведомо ложные показание, заключение эксперта, специалиста или неправильный перевод (ст.307 УК РФ), подкуп свидетеля, потерпевшего в целях дачи ими ложных показаний либо эксперта, специалиста в целях дачи ими ложного заключения или ложных показаний, а равно переводчика с целью осуществления им неправильного перевода (ст.309 УК РФ).

К категории информационных *объектов, связанных как с осуществлением противоправного информационного воздействия*, так и *с совершением преступления* следует относить различные информационные объекты, наиболее удачно характеризующиеся по способу осуществления деяния. При этом под противоправным информационным воздействием следует

определять цель совершаемого преступления, тогда как информационный объект, направленный на совершение преступления может рассматриваться как средство совершения преступления.

Особое место в числе информационных преступлений занимают киберпреступления, предметом[220] которых выступает компьютерная информация, под которой следует понимать сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи[221].

Здесь следует обратить особое внимание на то обстоятельство, что киберпреступления являются более широким понятием чем преступления в сфере компьютерной информации. Так, по мнению Т.Л. Тропиной, «под киберпреступностью понимается совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей и против компьютерных систем, компьютерных сетей или компьютерных данных[222]. Таким образом, понятие киберпреступности охватывает преступления, где современные информационные технологии выступают не только в качестве объекта или предмета преступления, но также орудия и средства его совершения.

Поскольку объектом Гл. 28 УК РФ выступает компьютерная информация, следует иметь в виду, что, согласно Закону «Об информации» под электронным документом понимается документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах. Итак, компьютерная информация по сути своей является электронным документом, хотя и связанным с материальным носителем, но невозможным к восприятию человеком без использования технологических средств.

---

[220] Жарова А.К., Елин В.М. О выделении информационных объектов в самостоятельную категорию объекта преступления // Труды Института государства и права Российской академии наук. 2009. № 5. С. 205-229.

[221] Ст. 272 УК РФ

[222] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Дис.... канд. юрид. наук. Владивосток, 2005. С. 36.

При сравнении российского законодательства [223] с нормами Конвенции о киберпреступности[224] ETS # 185 (также используется название «Конвенции о преступлениях в сфере компьютерной информации») обращает на себя внимание то обстоятельство, что наша страна не является ее участником по ряду причин:

- ограниченное количество составов преступлений в сфере киберпреступности;
- ограниченный состав стран-участниц Конвенции о киберпреступности;
- кабальные условия участия стран в данной Конвенции, связанные в первую очередь с положениями ст. 32-b, предусматривающей без согласия суверенного государства-участника как возможность доступа к общедоступным (открытому источнику) компьютерным данным независимо от их географического местоположения, так и возможность получения доступа через компьютерную систему на своей территории к компьютерным данным, хранящимся на территории другой стороны.

Однако следует иметь в виду, что европейская практика борьбы с преступлениями в компьютерной сфере является результатом практической деятельности Интерпола, в котором с 1991 года функционирует автоматизированная информационно – поисковая система, в основе которой находится классификатор методов совершения компьютерных преступлений в соответствии с Кодификатором Генерального секретариата Интерпола. Выделяется шесть классов и около трех десятков основных методов совершения компьютерных преступлений, причем их количество непрерывно пополняется.

По всей видимости, указанный подход в практике борьбы с компьютерными преступлениями в настоящее время является основным, о чем косвенно свидетельствует и положения ст. 3 Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации[225], которыми раскрываются составы уголовно-наказуемых деяний.

---

[223] См. Раздел V «Международное сотрудничество в области развития информационного общества» Стратегии развития информационного общества в Российской Федерации

[224] Convention on cybercrime. ETS # 185 (Budapest, 23.XI.2001)

[225] Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации. Заключено в г. Минске 01.06.2001 // Бюллетень международных договоров. 2009. № 6. С. 12 - 17.

Конвенционально предусматривается выделение четырех видовых объектов в структуре киберпреступности, к которым относятся:

- общественные отношения в сфере конфиденциальности, целостности и доступности компьютерных данных и систем;
- общественные отношения в сфере использования компьютерных средств;
- общественные отношения в сфере содержания данных;
- общественные отношения в сфере авторского права и смежных прав.

Преступления первой категории коррелируются с составами преступлений, предусмотренных российским законодательством:

- неправомерный доступ к компьютерной информации (ст. 272 УК РФ);
- создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);
- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274);
- незаконный оборот специальных технических средств, предназначенных для негласного получения информации (ст. 138.1 УК РФ);

Поскольку, под категорию преступлений с использованием компьютерных средств в Конвенции подпадают подлог с использованием компьютерных технологий и мошенничество с использованием компьютерных технологий, постольку следует соотнести их с соответствующими нормами российского права.

Новеллой российского законодательства является включение в состав уголовно-наказуемых деяний мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ), либо мошенничества с использованием платежных карт (159.3 УК РФ)[226]. При этом обращает на себя внимание то обстоятельство, что диспозиция ч. 1 ст. 159.6 УК РФ в точности совпадает с определением данного преступления, изложенным в Конвенции. Можно полагать, что дословное воспроизведение в нормах российского законодательства диспозиции мошенничества в сфере компьютерной информации, предлагаемой Конвенцией № 185, однозначно свидетельствует о том, что Российская Федерация, несмотря на категорический отказ от

[226] ФЗ от 29.11.2012 № 207-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации" // СЗ РФ, 03.12.2012, № 49, ст. 6752,

участия в Конвенции о киберпреступности, de facto является участником международных интеграционных процессов в данной сфере.

К сожалению, отнесение указанных составов к главе 21 УК РФ, видовым объектом которой являются отношения в сфере собственности, представляется не совсем правильным, поскольку исключение информации из перечня объектов гражданских правоотношений с 01 января 2008 года породило ряд гражданско-правовых последствий, о которых говорилось в § 2.2. настоящего исследования. В разделе правонарушений Конвенции, связанных с содержанием информации, предусматривается уголовная ответственность за производство, предложение (предоставление в пользование), распространение (передачу) и приобретение детской порнографии через компьютерную систему для себя или для другого лица, а также владение детской порнографией, находящейся в компьютерной системе или на носителях компьютерных данных.

При этом, в отличие от положений ст.ст. 242, 242-1 УК РФ понятие "детская порнография" раскрывается как участие несовершеннолетнего (либо лица, кажущегося несовершеннолетним) в откровенных сексуальных действиях, а также реалистические изображения несовершеннолетнего лица, участвующего в откровенных сексуальных действиях. Кроме того, конвенцией предусмотрена ответственность за владение детской порнографией, находящейся в компьютерной системе или на носителях компьютерных данных, в то время как ст. 242-1 УК РФ предусматривается ответственность лишь за изготовление, приобретение, хранение и (или) перемещение через Государственную границу Российской Федерации в целях распространения, публичной демонстрации или рекламирования либо распространение, публичная демонстрация или рекламирование материалов или предметов с порнографическими изображениями несовершеннолетних.

И, наконец, правонарушения, связанные с нарушением авторского и смежного прав отсылают нас к международным актам в данной сфере, таким как Соглашение о торговых аспектах прав интеллектуальной собственности, Договору об авторском праве Всемирной организации интеллектуальной собственности (ВОИС) и др. В российском уголовном законодательстве содержатся ст.ст. 146, 147, 180, 183, УК РФ, осуществляющие защиту правоотношений в данной сфере.

При это следует иметь в виду, что Конвенция предусматривает параллельное развитие материального и процессуального законодательства, однако в нашей стране практически отсутствуют правовое нормы как об электронном документе, так и о его процессуальной значимости., кроме того, обращает на себя внимание то обстоятельство, что с включением в нормы УК РФ ст.ст. 159.3 и 159.6 УК РФ, наша страна практически в полном объеме воспроизвела нормы Конвенции о материальном праве, что исключает в дальнейшем возможность использования международного опыта.

В результате сложилась ситуация, когда ряд диспозиции статей УК РФ практически дословно повторяет нормы указанной Конвенции (например ч. 1 ст. 159.6 УК РФ соотносится с р. 2 ч.1, гл. 2), ряд составов преступлений достаточно близок (ст. ст. 272 – 274 УК РФ, 138.1 УК РФ соотносится с р.1, ч. 1, гл.2), ряд составов можно соотнести концептуально (ст.ст. 242, 242-1, 242-2 и 146, 147 УК РФ соотносится с р. 3 и 4 ч.1. гл.2).

Кроме того, существует значительное количество отдельных составов преступлений (не менее 50), связанных с информационными технологиями, которые неравномерно распределяются по Особенной части УК РФ, и в которых информационные либо компьютерные технологии выступают в качестве предмета, орудия или средства совершения преступлений.

Однако, в отличие от норм Конвенции, где четко прослеживается родовой объект преступления, с дальнейшим подразделением его на ряд видовых и непосредственных объектов, в УК РФ имеет место единичный видовой объект данной отрасли, связанный с «Преступлениями в сфере компьютерной информации (гл. 28 УК РФ). Отсутствие четкой и структурированной системы преступлений данной категории является фатальным для условий уголовного права, поскольку нарушается логическая цепочка между объектом преступления (родовым, видовым и непосредственным), и общественно-опасными последствиями. Правовыми последствиями нарушения выступает ряд обстоятельств: информационные технологии становятся в лучшем случае дополнительным или факультативным объектом преступлений; возникает проблема отсутствия материальных последствий причинения вреда (например: составы мошенничества с использованием платежных карт (ст. 159.3. УК РФ) и мошенничества в сфере компьютерной информации (ст. 159.6. УК РФ));

информационные технологии не квалифицируются как предмет, орудие или средства совершения преступлений и т.д.

То обстоятельство, что понятие «компьютерного преступления», напрямую связанно с понятием «электронного документа» напрямую связывает данную сферу с рядом проблем:

- излишняя декларативность и «размытость» норм международного права в данной сфере;
- значительная затрудненность контроля на национальном уровне за обращением информации в международных информационных системах;
- отсутствие правового статуса электронного документа;
- отсутствие правовых норм, осуществляющих регулирование в данной сфере;
-проблематика согласования аспектов правового и технического регулирования защиты электронного документа;
- отсутствие реквизитов электронного документа.

На основе проведенного анализа представляется возможным дать авторское определение понятий «Информационные преступления» и «Компьютерные преступления».

При этом под **информационными преступлениями следует понимать совершение запрещенных уголовным кодексом деяний, имеющих своей целью причинение вреда в сферах реализации информационных прав, применения информационных технологий и обеспечения защиты информации; деяний с использованием вредоносных информационных объектов; а также с использованием информации (информационных технологий) в качестве орудия, средства или способа совершения преступления, объектом и предметом которых выступает информация и информационные отношения.**

Представляется необходимым окончательное признание информации одним из признаков материи, законодательное раскрытие понятий «вредоносной информации», «информационных объектов», принятие законодательных и иных мер, направленных на формирование правового режима ряда категорий информации ограниченного доступа.

При этом, в качестве первого шага представляется выделение в уголовном праве родового объекта состава преступлений – общественные отношения в

сфере информационных технологий. Видовыми объектами при этом могут выступать общественные отношения в сферах:

- компьютерных технологий, программ и информации;
- функционирования систем хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
- неправомерного использования компьютерной информации;
- защиты компьютерной информации;
- содержания компьютерной информации.

Таким образом, под **компьютерными преступлениями следует понимать запрещенные уголовным кодексом деяния, совершенные с применением или использованием компьютерной информации (технологии), причиняющих вред охраняемым законом общественным отношениям в сфере информационных систем и технологий, либо направленные на нарушение функционирования систем хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.**

Уже сейчас можно с уверенностью сказать, что несмотря на молодость информационного права оно находится в тесной взаимосвязи с Российским уголовным правом, в течение длительного времени развивавшего систему борьбы с информационными преступлениями, причем эта система является достаточно упорядоченной и взвешенной, соотносится с положениями и информационного права и вызовами современности.

В уголовном праве сложилась система составов, где информация выступает в качестве предмета преступления, причем классификацию преступлений можно производить как по категориям информации, так и по категориям деяний в отношении нее.

Несмотря на категорический отказ от участия в Киберконвенции ETS # 185, фактическое развитие российского уголовного законодательства развивалось по европейскому пути, причем можно с уверенностью сказать о том, что данный подход к настоящему времени практически полностью исчерпался, в связи с чем необходимо уделить внимание формированию концептуального подхода к борьбе с информационными преступлениями в будущем.

Глава 3. Правовое регулирование некоторых сфер информатизации в России и за рубежом

3.1. Защита приватности и персональных данных в законодательстве России и США

Дуалистичность подхода к обеспечению безопасности персональных данных в Российской Федерации определяется тем обстоятельством, что к началу активной организационно-правовой деятельности Евросоюза в данной сфере в России уже было выработано отношение к данной проблеме.

Европейский подход к защите персональных данных напрямую связывают с принятием Directive 95/46/EC of the European Parliament and of the Council[227]. Дальнейшее развитие получило в Directive 2002/58/EC of the European Parliament and of the Council[228], которая применяется в отношении обработки персональных данных в связи с предоставлением общедоступных услуг электронной связи в сетях связи коллективного доступа.

Между тем, в нашей стране Конституционный принцип невмешательства в личную жизнь граждан имеет глубокие правовые традиции. Уже в Конституции 1937 года[229] закреплено право неприкосновенности жилища граждан и тайны переписки. Статья 40 Конституции 1978 года определяла уже права граждан на неприкосновенность его частной жизни, на тайну переписки, телефонных переговоров, телеграфных и иных сообщений.[230] Значимость данной категории правоотношений подтверждается включением в Уголовный кодекс 1961 года статьи 135, предусматривающей ответственность за

[227] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Pab. in Official Journal № L 281, 23.11.1995, P. 31. // СПС Консультант плюс

[228] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).. Pab. in Official Journal № L 201, 31.7.2002, P. 37.// СПС Консультант плюс

[229] Постановление Чрезвычайного XVII Всероссийского Съезда Советов от 21.01.1937 «Об утверждении Конституции (Основного Закона) Российской Советской Федеративной Социалистической Республики» (вместе с Конституцией) // СПС «Консультант плюс»

[230] Конституция (Основной Закон) Российской Федерации – России (принята ВС РСФСР 12.04.1978) // СПС «Консультант плюс»

нарушение тайны переписки, телефонных переговоров и телеграфных сообщений граждан[231].

В новейшей истории конституционный принцип неприкосновенности частной жизни, личной и семейной тайны, тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений определен ст. 23 Конституции Российской Федерации232 и защищается нормами уголовного и гражданского законодательства.

О пристальном внимании к данной категории информации ограниченного доступа свидетельствует постоянная корректировка законодательства, в частности, - дополнение Гражданского кодекса Российской Федерации ст. 152.2, прямо запрещающей без согласия гражданина сбор, хранение, распространение и использование любой информации о его частной жизни[233]. Тем самым представлен механизм с помощью которого граждане могут иметь секреты друг от друга и от самого государства в личной и семейной жизни.

Право на личную и семейную тайну принадлежит каждому человеку от рождения. Оно является его естественным правом и причисляется к нематериальным благам, направленным на неприкосновенность внутреннего мира человека и его интересов. Особенность осуществления этого права состоит в том, что определяются не границы его осуществления, а границы вторжения посторонних лиц в личную сферу индивида.

Право на неприкосновенность частной жизни складывается из ряда норм различных отраслей права. В содержание этих прав входит охрана тайны личной жизни лица, оглашение сведений о которых это лицо по тем или иным причинам считает нежелательным (например, тайна завещания, усыновления, врачебного диагноза, денежного вклада, дневниковых записей и т.д.)[234]. Право на частную жизнь гарантируется такими конституционными и иными правовыми установлениями, как неприкосновенность жилища, возможность беспрепятственного общения с другими людьми посредством

---

[231] Закон РСФСР от 27.10.1960 Об утверждении Уголовного кодекса РСФСР (вместе с "Уголовным кодексом РСФСР") // СПС «Консультант плюс»

[232] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // http://www.pravo.gov.ru

[233] Введена ФЗ от 02.07.2013 № 142-ФЗ "О внесении изменений в подраздел 3 раздела I части первой Гражданского кодекса Российской Федерации" // Собрание законодательства РФ, 08.07.2013, № 27, ст. 3434

[234] Права человека. Учебник для вузов // Под ред. Е.А. Лукашевой. М., 2001. С. 146.

почты, телеграфа, телефона и других средств коммуникации, право распоряжаться семейным бюджетом, личной и частной собственностью, денежными вкладами, тайна которых гарантируется законом.

При этом можно наблюдать соотносимость правовых институтов неприкосновенности частной жизни, личной и семейной тайны с международными нормами о правах человека. Так, ст. 12 Всеобщей декларации прав человека определяет, что никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию[235]. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств. Положениями Международного пакта о гражданских и политических правах человека определено, что никто не может подвергаться произвольному или незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию[236].

Следует иметь в виду, что сущность понятий личной и семейной тайны не имеет официального толкования, несмотря на то обстоятельство, что понятие "личная тайна" употребляются в 5-и нормативных актах, а "семейная тайна" - еще в 3-х[237], что следует связывать с необходимостью регулировать отношения между людьми в частной сфере в основном нормами нравственности[238].

При этом право на неприкосновенность частной жизни складывается из двух составляющих:

- обеспечение человеку возможности находиться вне службы, вне производственной обстановки, вне общественного окружения в состоянии известной независимости от государства и общества;

---

[235] Всеобщая декларация прав человека. Принята Генеральной Ассамблеей Организации Объединенных Наций 10 декабря 1948 года.

[236] Международный пакт о гражданских и политических правах. Открыт для подписания, ратификации и присоединения 19.12.1966 Резолюцией 2200 А (XXI) Генеральной Ассамблеи ООН. Пакт вступил в силу 23.03.1976.

[237] Лопатин В.Н. Правовая охрана и защита служебной тайны // Государство и право. 2000. № 6. С. 85.

[238] Петрухин И.Л. Частная жизнь (правовые аспекты) // Государство и право. 1999. № 1. С. 64.

- осуществление контроля за информацией о самом себе и возможность препятствовать разглашению информации личного, в особенности - интимного характера.

Таким образом, обоснованным представляется соотнесение российского понятия «тайны частной жизни, личной и семейной тайны» с американскими терминами «confidentiality or privacy», раскрывавшимися в работе Samuel D. Warren and Louis D. Brandeis «The Right to Privacy»239. При этом в российской общественном сознании под privacy в первую очередь понималось the right to be let alone или secrecy, or the option to conceal any information from others (скрытность как вариант сокрытия информации от других). Особенностью общественного сознания выступает признание за государством права контролировать в случаях обеспечения безопасности государства, общества и граждан принципа states at privacy (vs. states of privacy), т.е. «государства в частной жизни» (а не «государство для частной жизни»).

Толкование Конституционного суда не проясняет вопрос о содержании данной категории информации: «Право на неприкосновенность частной жизни, личную и семейную тайну означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера; в понятие "частная жизнь" включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если носит непротивоправный характер,…лишь само лицо вправе определить, какие именно сведения, имеющие отношение к его частной жизни, должны оставаться в тайне, а потому и сбор, хранение, использование и распространение такой информации, не доверенной никому, не допускается без согласия данного лица». Однако Конституционный суд Российской Федерации указывает на обязательное условие сохранения тайны – непротивоправный характер действий субъекта[240].

239 The Right to Privacy //Samuel D. Warren and Louis D. Brandeis //Harvard Law Review. Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-2

[240] Определение Конституционного Суда РФ от 28.06.2012 N 1253-О «Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137

Что характерно, прослеживается схожесть подходов российского суда и Европейского суда по правам человека в вопросе « в защите отдельного лица от своевольного вмешательства государственных властей»[241].

Исходя из предписаний ч.1 ст. 23 и ч. 1 ст. 24 Конституции Российской Федерации, конфиденциальным характером обладает любая информация о частной жизни лица, а потому она во всяком случае относится к сведениям ограниченного доступа[242].

В толковых словарях русского языка слово "частный" противопоставляется словам "общественный", "государственный". При этом в юридической науке под частной жизнью понимается область личных, интимных, семейных, бытовых и иных отношений людей, "которая контролируется самим индивидом, т.е. свободна от внешнего воздействия"[243]. М.В. Баглай определяет, что частная жизнь "это - своеобразный суверенитет личности, означающий неприкосновенность его "среды обитания"[244].

Исторически неприкосновенность частной жизни соотносится с понятием "privacy" ("приватность"), попытку раскрыть которое впервые предпринята С. Уорреном и Л. Браидейсом, которые определяли его как "право быть оставленным в покое"[245], при том, что "напряженность и сложность жизни, присущие развивающейся цивилизации, приводят к необходимости иметь убежище от внешнего мира, так что уединение и приватность становятся для человека более значимыми".

По мнению А. Вестина, существуют следующие формы приватности[246]:

- "уединение", состояние, в котором человек избавлен от наблюдения со стороны других;

- "интимность", замкнутое общение, предполагающее контакт с узким кругом лиц;

Уголовного кодекса Российской Федерации», Определение Конституционного Суда РФ от 09.06.2005 N 248-О «Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом "б" части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации» // СПС Консультант плюс

[241] Постановление Европейского суда по правам человека от 28 мая 1985 года "Абдулазис, Кабалес и Балкандали против Соединенного Королевства" ("Abdulaziz, Cabales et Balkandali v. United Kingdom"// СПС Консультант плюс

[242] Определения Конституционного Суда Российской Федерации от 9 июня 2005 года № 248-О, от 26 января 2010 года № 158-О-О и от 27 мая 2010 года № 644-О-О // СПС Консультант плюс

[243] Частная жизнь (правовые аспекты) // Отв. ред. Е.А. Лукашева. С. 146; Петросян М.Е. Что такое неприкосновенность частной жизни? // Правозащитник. 1995. № 1. С. 49.

[244] Баглай М.В. Конституционное право Российской Федерации. М., 2005. С. 185.

[245] Louis Brandeis & Samuel Warren *The Right to Privacy*, // "Harvard Law Review", 1890. 12.15.

[246] Westin A.F. Privacy and freedom. N.Y.: Autheneum, 1970. P. 39.

- "сдержанность", наличие психологического барьера между индивидом и окружающими людьми, который поддерживается обеими сторонами;

- "анонимность", состояние, когда человек не имеет желания быть узнанным в тех или иных ситуациях.

Неприкосновенность частной жизни означает запрет для общества, государства и его органов, должностных и иных лиц вмешиваться в личную жизнь граждан (в том числе право последних на свои личные и семейные тайны), наличие правовых механизмов и гарантий защиты своей чести и достоинства от всевозможных посягательств.

С точки зрения специалистов в области конституционного права, частную жизнь можно определить как физическую и духовную сферу, которая контролируется самим индивидом, т.е. сферу, которая свободна от внешнего воздействия[247]. Законодательство не может вторгаться в нее, а потому категория "частная жизнь" не имеет юридического содержания; право устанавливает лишь пределы ее неприкосновенности ("приватности") и пределы допустимого вмешательства.

В юридической науке под частной жизнью понимается область личных, интимных, семейных, бытовых и иных отношений людей, "которая контролируется самим индивидом, т.е. свободна от внешнего воздействия"[248].

М.В. Баглай определяет, что частная жизнь "это - своеобразный суверенитет личности, означающий неприкосновенность его "среды обитания"[249]. К сведениям о частной жизни лица относят информацию, непосредственно связанную с конкретным человеком (факты его биографии, номинативные (назывные) данные, национальность, место жительства, сведения о заболеваниях, информация о семейной жизни, привычках, увлечениях, нравственных, политических, сексуальных и религиозных пристрастиях), что составляет большую часть циркулирующей в обществе информации[250].Задача закона состоит только в том, чтобы исчерпывающим образом зафиксировать процедуру вторжения в частную жизнь человека в интересах борьбы с преступностью, охраны здоровья и безопасности других

[247] Права человека: Учебник // Под ред. А.Н. Головистиковой, Л.Ю. Грудицына. М., 2006. С. 121.
[248] Частная жизнь (правовые аспекты) / Отв. ред. Е.А. Лукашева. С. 146; Петросян М.Е. Что такое неприкосновенность частной жизни? // Правозащитник. 1995. № 1. С. 49.
[249] Баглай М.В. Конституционное право Российской Федерации. М., 2005. С. 185.
[250] Хендрикс А., Хэйден Т., Новик Д.Д. Ваше право на неприкосновенность частной жизни: Пособие по защите законных прав в информационном обществе / Пер. с англ. М.Е. Петросян. СПб., 1996

людей, т.е. в случаях, признаваемых правомерными в цивилизованных демократических государствах.

По мнению Б.Н. Топорнина, под личной тайной понимается право индивида определять свое поведение в обществе, самостоятельно решать, кому и в каком объеме доверить ту или иную информацию, и требовать от третьих лиц соблюдения этих прав. Это никому не доверенная информация или доверенная лицам, обязанным в силу своих профессиональных обязанностей хранить тайну: врачам, адвокатам, нотариусам, священникам[251].

К сведениям о частной жизни лица ряд авторов также считает возможным отнести тайну творчества и общения, тайну семейных и интимных взаимоотношений, тайну жилища, дневников, личных бумаг, тайну почтово-телеграфной корреспонденции и телефонных переговоро[252]в. Право на частную жизнь выражается в свободе общения между людьми на неформальной основе в сферах семейной жизни, родственных и дружеских связей, интимных и дружеских связей, интимных и личных отношений.

Сведения о частной жизни лица (личные тайны), защищенные правовыми запретами, адресованные тем, кому эти сведения по необходимости доверены, лежат в основе профессиональных тайн. Существует также мнение о том, что врачебная, адвокатская, переписки, усыновления и прочие тайны, в сущности, и образуют право гражданина на неприкосновенность его частной жизни[253].

При этом профессиональные тайны как обобщенный правовой институт чаще всего представляют собой информацию, защита от несанкционированного распространения которой является обязанностью субъекта в силу выполнения им профессиональных функций. В отраслевое законодательство, как правило, закладывается обязанность нераспространения сведений о пациентах (клиентах), которая является неотъемлемой характеристикой самой профессии[254].

---

[251] Комментарий Конституции Российской Федерации / Под ред. Б.Н. Топорнина. М.: Юрист, 1997. С. 202.
[252] Государственная тайна и ее защита в Российской Федерации: Учебное пособие // Под общ. ред. М.А. Вуса и А.В. Федорова. СПб., 2007. С. 146.
[253] Петрухин И.Л. Личные тайны (человек и власть). М., 1998.
[254] См., например: ст. 61 Основ законодательства Российской Федерации об охране здоровья граждан от 22 июля 1993 года № 5487-1, ст. 16 Основ законодательства Российской Федерации о нотариате № 4462-1, утв. ВС РФ 11 февраля 1993 года или ст. 8 ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации" от 31 мая 2002 года № 63-ФЗ.

В теории гражданского права также обоснована точка зрения о том, что право на личную и семейную тайну связывается с возможностью определять личное поведение в индивидуальной жизнедеятельности[255].

При этом всю совокупность тайн, относимых к сведениям о частной жизни лица, можно подразделить на тайны, не доверяемые никому, и тайны, доверяемые кругу лиц, определяемому личностью. К указанному кругу доверенных лиц можно отнести представителей определенных профессий, осуществляющих защиту прав и законных интересов граждан (профессиональные тайны), что, в свою очередь, позволяет подразделить сведения, составляющие право на личную и семейную тайну, на:

- сведения, переданные лицом добровольно другому лицу и не подлежащие разглашению третьим лицам (конфиденциальная информация), которые характеризуют наличие доверительных отношений между лицом, которое имеет тайну, и лицами, которым он ее доверяет;

- сведения, передаваемые третьим лицам с неизбежным использованием услуг (помощи) третьих лиц, закрепленные на материальном носителе или выраженные в иной объективной форме, которые передаются адресату через третьих лиц путем оказания услуг связи (например, электронная корреспонденция, сотовая или городская телефонная связь);

- конфиденциальные сведения о лице (т.е. сведения, которые это лицо само не считает нужным разглашать), полученные без его ведома путем целенаправленного сбора. Данный вид сведений может быть предметом деятельности властных структур государства. Эти тайны никому не доверены, однако имеют важное общественно-политическое значение. Сведения могут быть получены помимо воли лица или под угрозой наказания или вследствие того, что гражданин может лишиться каких-то благ (например, сведения, полученные в результате оперативно-розыскных действий)[256].

Параллельно с развитием законодательства о защите частной жизни лица предпринимается комплекс мер по защите персональных данных, что можно связать с положениями Конвенции Совета Европы о защите

[255] Гражданское право. Учебник для вузов. Ч. 1 / Под ред. Ю.К. Толстого, А.П. Сергеева. М., 1996. С. 278.
[256] Права человека: Учебник // А.Н. Головистикова, Л.Ю. Грудцына. М., 2006. С. 125.

физических лиц при автоматизированной обработке персональных данных[257]".

Построение системы правового регулирования режима персональных данных в Российской Федерации можно отнести к 7 ноября 2001 года, когда Россия подписала Конвенцию о защите физических лиц при автоматизированной обработке персональных данных[258].

Конвенция ратифицирована в 2005году принятием Федерального Закона «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»[259].

С принятием Закона «О персональных данных»[260] принимается комплекс организационно-техническим и правовых мер, направленных на обеспечение безопасности персональных данных.

С этого момента можно проследить определённое смешение понятий «персональные данные» и «тайна личной жизни» в ряде нормативных актов и в научной литературе. Так, Президентский Указ № 188, определивший Перечень сведений конфиденциального характера[261], соотносит понятие сведений о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющих идентифицировать его личность, с понятием персональных данных, определение которых совпадает с конвенциональным, закреплено в Федеральном законе и под которым следует понимать любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Существует обоснованное мнение[262] о том что российская дефиниция персональных данных затрудняет применение этого термина на практике, так как, с одной стороны, позволяет любую информацию, создаваемую

---

[257] Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» // СЗ РФ, 26.12.2005, № 52 (1 ч.), ст. 5573

[258] Заключена в г. Страсбурге 28.01.1981 года

[259] Федеральный закон от 19.12.2005 № 160-ФЗ «"О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» // СЗ РФ, 26.12.2005, № 52 (1 ч.), ст. 5573 // СПС Консультант плюс

[260] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ 31.07.2006, № 31 (1 ч.), ст. 3451

[261] Утвержден Указом Президента Российской Федерации № 188 от 6 марта 1997 г. // ССППС Консультант плюс

[262] Дупан А.С., Титова С.В., Жулин А.Б., Жарова А.К., Елин В.М., Бикбулатов Т.И., Бикбулатова Ю.С., Римша Д. Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети интернет /Под редакцией А.С. Дупан (Гутниковой). Москва, 2016.

человеком или о человеке, рассматривать как персональные данные (со всеми вытекающими последствиями в виде необходимости соблюдать требования, предъявляемые операторам персональных данных), а с другой стороны, не позволяет, исходя из буквального толкования, применять нормы о персональных данных к случаям, когда с помощью данных идентифицируется не конкретное лицо, а устройство (компьютер, мобильный телефон и т.д.), которым пользуется физическое лицо.

Стремление к участию в европейских интеграционных процессах оставляет за рамками внимания то обстоятельство, что персональные данные не являются равнозначными сведениям о частной жизни лица, по мнению ряда зарубежных исследователей, включая в себя сведения не только privacy, но и publicy. Также очень интересным представляется то обстоятельство, что в Конституциях ряда европейских стран (Англия, Франция, Германия[263]) не содержится принципа неприкосновенности частной жизни, охраны личной и семейной тайны. Таким образом, просматривается несоответствие правовых норм России и развитых стран Европы в данной сфере.

Практическая реализация защиты персональных данных по компетенциям в Российской Федерации связана с деятельностью Федеральной службы по техническому и экспортному контролю[264], Федеральной службы безопасности Российской Федерации[265], Министерства связи и массовых коммуникаций Российской Федерации.

Дополнительно можно выделить отраслевые подходы, например Центробанка, МНС Российской Федерации и т.д., поскольку достаточно произвольное определение персональных данных смешивает их со сведениями, относящимися к банковской, налоговой тайне, иным категориям информации ограниченного доступа.

---

[263] Конституции стран размещены в СПС Консультант плюс

[264] Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»//СПС Консультант +; Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // РГ, № 136, 26.06.2013

[265] «Типовой регламент проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Утв. ФСБ России 08.08.2009 № 149/7/2/6-1173 // СПС Консультант +; «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации». Уутв. ФСБ РФ 21.02.2008 № 149/54-144) // СПС Консультатнт плюс

Взаимосвязь между тайной частной жизни и персональными данными закреплена Указом Президента Российской Федерации N 188 "Об утверждении Перечня сведений конфиденциального характера"[266]. Указ производит легальную классификацию сведений конфиденциального характера, которые выступают значительной составляющей информации ограниченного доступа и выделяет персональные данные как самостоятельную категорию конфиденциальной информации ограниченного доступа. Указ определяет персональные данные как сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность.

Персональные данные как категория информации ограниченного доступа связана с тем, что Закон "Об информации, информационных технологиях и о защите информации" подразделяет информацию по категориям доступа к ней на общедоступную и информацию ограниченного доступа, причем доступ к информации может быть ограничен только федеральными законами. Основаниями ограничения доступа к информации определены[267]: защита основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечение обороны страны и безопасности государства, в отношении информации, для которой обязательным является соблюдение режима конфиденциальности. В отношении информации ограниченного доступа обязательным является соблюдение конфиденциальности информации.

При этом в отношении персональных данных как подмножества информации ограниченного доступа, характерен ряд признаков:

- под персональными данными следует понимать специфическую информацию, скрываемую субъектом от других членов общества, в силу необходимости решения специфических задач обеспечения информационной безопасности личности, общества и государства;

- обязательным условием ограничения доступа к персональным данным является требование федерального закона;

[266] Указ Президента Российской Федерации "Об утверждении Перечня конфиденциального характера" № 188 от 06.03.1997 // СПС "КонсультантПлюс".
[267] Ст.9 ФЗ "Об информации, информационных технологиях и о защите информации" // СПС "КонсультантПлюс".

- персональные данные характеризуются единством составляющей информации и правового режима ограничения доступа к ней;

- в отношении персональных данных применяются специальные правовые режимы, основным назначением которых является решение задачи защиты информации;

- реализация защиты информации в отношении персональных данных состоит в соблюдении конфиденциальности такой информации, в то время -- как для общедоступной информации - в реализации права на доступ к информации.

Параллельно с развитием законодательства о защите частной жизни лица предпринимается комплекс мер по защите персональных данных, что можно связать с положениями Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных[268].

Регулирование отношений, связанных с обработкой персональных данных с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств осуществляется в соответствии с нормами закона «О персональных данных»[269].

Согласно Постановлению Правительства Российской Федерации № 1119[270] следует различать 3 типа угроз безопасности персональных данных как условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

В сочетание актуальных угроз различных типов порождает необходимость обеспечения 4-х уровней защищенности персональных данных:

---

[268] Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» // СЗ РФ, 26.12.2005, № 52 (1 ч.), ст. 5573

[269] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ", 31.07.2006, № 31 (1 ч.), ст. 3451

[270] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // "Собрание законодательства РФ", 05.11.2012, № 45, ст. 6257

- для обеспечения 4-го уровня защищенности персональных данных необходимо обеспечение безопасности помещений, в которых размещена информационная система; обеспечение сохранности носителей персональных данных; утверждение документа, определяющего перечень лиц с разрешенным доступом; использование сертифицированных средств защиты информации.

- для обеспечения 3-го уровня защищенности персональных данных дополнительно, помимо выполнения требований 4-го уровня, необходимо назначение работника, ответственного за обеспечение безопасности персональных данных в информационной системе.

- для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных дополнительно, помимо выполнения требований 3-го уровня, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

- для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах дополнительно, помимо выполнения требований 2-го уровня, необходимо выполнение требований автоматической регистрации в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе; а также создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности. Практическая реализация защиты персональных данных возложена на Федеральную службу по техническому и экспортному контролю (ФСТЭК России), которая является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, специальные и контрольные функции в области государственной безопасности по вопросам обеспечения защиты информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители

информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации[271].

ФСТЭК России предлагает Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных[272], согласно которой угрозы классифицируются:

- по виду защищаемой информации;
- по видам возможных источников угроз;
- по типу информационных систем персональных данных, на которые направлена реализация угроз;
- по способу реализации угроз;
- по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с персональными данными;
- по используемой уязвимости;
- по объекту воздействия.

Построение подклассов и определение связей между ними приводит к построению Базовой модели угроз безопасности персональных данных.

На основании детального описания угроз, связанных с утечкой персональных данных по техническим каналам, определяемых Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных разработана и применяется Методика определения актуальных угроз безопасности персональных данных[273].

При этом учитывается возможность утечки персональных данных по техническим каналам либо за счет несанкционированного доступа с использованием соответствующего программного обеспечения.

С использованием данных о классе информационных систем по обработке персональных данных и составленного перечня актуальных угроз, формулируются конкретные организационно-технические требования по защите информационных систем от утечки информации по техническим

[271] Указ Президента РФ от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» // "Собрание законодательства РФ", 23.08.2004, № 34, ст. 3541

[272] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. утв. ФСТЭК РФ 15.02.2008 // СПС Консультант плюс

[273] Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утв. ФСТЭК РФ 14.02.2008 // СПС Консультант плюс

каналам, от несанкционированного доступа и осуществляется выбор программных и технических средств защиты информации.

К конкретным мерам по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят[274]:

- идентификация и аутентификация субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;

- ограничение программной среды;

- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

- регистрация событий безопасности;

- антивирусная защита;

- обнаружение (предотвращение) вторжений;

- контроль (анализ) защищенности персональных данных;

- обеспечение целостности информационной системы и персональных данных;

- обеспечение доступности персональных данных;

- защита среды виртуализации;

- защита технических средств;

- защита информационной системы, ее средств, систем связи и передачи данных;

- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

- управление конфигурацией информационной системы и системы защиты персональных данных.

Следует иметь в виду, что именно в интересах обеспечения безопасности персональных данных в Российской Федерации, приняты

[274] Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»// СПС Консультант плюс

изменения в действующее законодательство, связываемые с «правом на забвение». Правовая норма включает в себя обязанности оператора поисковой системы прекратить выдачу сведений об указателе страницы сайта в сети "Интернет", позволяющих получить доступ к информации о заявителе, распространяемой с нарушением законодательства Российской Федерации, являющейся недостоверной, а также неактуальной, утратившей значение для заявителя в силу последующих событий или действий заявителя.

Несмотря на схожесть Российского и американского подходов к пониманию содержания «privacy» как "право быть оставленным в покое"[275], практическая реализация этого процесса в указанных странах кардинально отличается. Если исходить из того, что Российская Федерация пошла по европейскому пути в части защиты персональных данных и построила собственную модель защиты тайны личной жизни, то в США понятие «privacy» напрямую коррелируется с **Title 15 U.S. Code, Chapter 94 – "Privasy".**

Согласно § 6809 Nonpublic personal information[276] (непубличную персональную информацию) следует определять как личную финансовую информацию, полученную в результате выполнения работ для потребителя услуг финансового учреждения, либо в результате сделки с потребителем (финансовым учреждением) или иным способом. Финансовое учреждение обязано уважать частную жизнь своих клиентов и защищать безопасность и конфиденциальность непубличной личной информации этих клиентов, и обязано установить соответствующие стандарты для финансовых институтов, находящихся под их юрисдикцией относящиеся к административной, технической, физической деятельности, направленной на обеспечение безопасности и конфиденциальности записей о клиентах; защиты от любой предполагаемой угрозы или опасности безопасности или целостности таких записей, а также от несанкционированного доступа или использования документов или информации, которые могли бы привести к существенному вреду или неудобству для любого клиента.

Финансовое учреждение не может непосредственно или через любой филиал, раскрывать связанным с ним третьим лицам любую непубличную личную

[275] Louis Brandeis & Samuel Warren *The Right to Privacy*, // "Harvard Law Review", 1890. 12.15.
[276] https://www.law.cornell.edu/uscode/text/15/6801

информацию, если такое финансовое учреждение не предоставляет потребителю уведомление.

Использование понятия "privacy" (в качестве личной конфиденциальной информации в США) раскрывает основную специфику защиты информации именно в интересах сферы торговли. При этом Federal Trade commission (ФТК, Комиссия) осуществляет свою деятельность на основании Федерального Закона Privacy Act of 1974. ФТК вменяется в обязанность собирать и хранить информацию, выступать с законодательной инициативой, в т.ч. и по законам, не имеющим отношения к деятельности Комиссии, однако затрагивающим сферу защиты личной конфиденциальной информации, например: Children's Online Privacy Protection Act (COPPA), Family Educational Rights and Privacy Act.

The Privacy Act 1974 определяет ряд принципов обработки информации, в части:

- точности, полноты, актуальности и своевременности личной информации в файлах агентств;
- возможность доступа физических лиц к информации о себе;
- возможности реализации процедуры обжалования точности информации;
- определения совокупности гражданско-правовых механизмов защиты прав физических лиц;
- определения полномочия государственных органов в части обработки информации.

Положениями закона определена презумпция доступа граждан к информации и себе в государственных органах.

Механизм обработки обращений граждан определен документом «Правила освобождающие системы записей из определенных требований конфиденциальности» (**A citizen's guide on using the freedom of information act and the privacy act of 1974 to request government records**)[277]. Правилами определено, что регистрация информации физических лиц производится как по имени, так и по какому-либо регистрационному номеру, символу или другим идентификационным признакам.

[277] A citizen's guide on using the freedom of information act and the privacy act of 1974 to request government records // http://thomas.loc.gov/cgi-bin/cpquery/z?cp106:hr50.106.m

Исключения из требований о режиме конфиденциальности определены в 28 Положений Committee of the Federal Register Часть 16, подраздел E[278], определяющей порядок освобождений от обязательных требований Закона о конфиденциальности.

Federal Trade Commission (FTC) разрабатываются и предлагаются к принятию ряд законов, таких как Federal Trade Commission Act[279]; H.R.4366 - Personal Data Offshoring Protection Act of 2004[280]; H.R.4127 - Financial Data Protection Act of 2006[281]. Помимо этого, следует иметь в виду ряд нормативных актов, направленных на регулирование торговой деятельности (Fair Credit Reporting Act, Financial Services Modernization Act of 1999 и т.д.) которые затрагивают проблематику защиты личной конфиденциальной информации.

В интересах FTC разрабатываются и предлагаются к принятию ряд законопроектов (Bill), в соответствии с которыми персональные данные используются для осуществления коммерческой деятельности.

Указанные законопроекты представляют интерес с точки зрения предложений по официальному толкованию понятия «персональные данные», анализа различных точек зрения на сферу и механизмы правового регулирования данного института.

H.R.2368 - Data Privacy Act of 1997, - обеспечивает предоставление компьютерных интерактивных услуг рабочей группой, которая должна разработать добровольные руководящие принципы:

- ограничения сбора и использования для коммерческого маркетинга любой личной информации, полученной с использованием интерактивной компьютерной службы;
- сбора информации с использованием нежелательной коммерческой электронной почты.

Запрещает:

- коммерческое использование определенной информации о личности, полученной с использованием любой интерактивной сервиса без предварительного согласия человека;

[278] https://www.law.cornell.edu/cfr/text/28/part-16/subpart-E

[279] Вносился в Сенат неоднократно, 1979, 1982, 1983. Не прошел слушания в Сенате США // https://www.congress.gov/bill/98th-congress/senate-bill/1714/actions

[280] https://www.congress.gov/bill/108th-congress/house-bill/4366

[281] http://www.loc.gov/search/?in=&q=Financial+Data+Protection+Act+of+2006&new=true

- использование номера социального обеспечения любого человека посредством интерактивного компьютерного сервиса.

H.R.4366 - Personal Data Offshoring Protection Act of 2004, - закрепляет требования к коммерческим организациям информировать граждан в связи с передачей персональных данных граждан в зарубежных филиалы или субподрядчикам, расположенных в странах с адекватной системой защиты частной жизни.

Запрещает трансграничную передачу в страны, где защита недостаточна.

Создает личное право на иск за нарушение настоящего Закона. Уполномочивает государство, от имени своих жителей, осуществлять подачу исков в Федеральный суд за такие нарушения.

Поручает Федеральной комиссии по торговле сертифицировать страны по уровню защиты информации.

Требует сертификацию стран, законодательство которых соответствует требованиям Директивы Европейского Союза о защите данных, если такие законы не обеспечены должным образом.

S.1326 - Notification of Risk to Personal Data Act (2005- 2006), - формулирует требования к любому учреждению или частному лицу обладающему лицензированными компьютерными данными, содержащими конфиденциальную личную информацию:

- внедрить и поддерживать разумную безопасность процедур и практики для защиты конфиденциальной личной информации от несанкционированного доступа, уведомления, уничтожения, использования, изменения или раскрытия;
- уведомлять любого жителя США, чья сугубо личная информация была скомпрометирована.

H.R.4127 - Financial Data Protection Act of 2006, - вносит изменения в Fair Credit Reporting Act, определяет руководящие принципы для гарантий безопасности данных потребительского рынка. Определяет "consumer reporter" как организацию которая занимается регулярно сбором, анализом и предоставлением третьим лицам потребительских отчетов.

Определяет политику Конгресса в данной сфере.

В том, что касается отраслевого применения «privasy» в США, следует отметить жестко определяемое понятие в каждой из сфер, что отличает его от европейского, предельно лапидарного и неопределенного.

Так, Закон **Health Insurance Portability and Accountability Act**[282] (HIPPA) определяет Protected Health Information (PHI), как сведения, связанные с охватываемыми лицами (covered entities). К указанной информации относится любая информация о состоянии здоровья, оказании медицинской помощи, оплаты медицинской помощи, связанные с конкретной личностью. Отраслевое законодательство применяет два способа идентификации (деидентификации)[283]: как по использованию статистических методов, так и по наличию идентифицирующих признаков, к которым относятся: имена; телефонные номера; номера факсов; электронные адреса электронной почты; социальный номер; медицинский номер; номер медицинских бенефициаров; номера счетов; сертификат / лицензионные номера; идентификаторы автомобиля; идентификаторы устройств и серийные номера; universal resource локаторы (URL); IP- адрес; биометрические идентификаторы, в том числе пальцев и голосовых отпечатков; полное лицо фотографические изображения и любые сопоставимые изображения; и т.д.

Уголовное законодательство (**Title 18 § 1028 (D) (7) U.S.Code**) раскрывает термин: "средства идентификации" как любое имя или номер, который можно использовать по отдельности или в сочетании с любой другой информацией, чтобы идентифицировать конкретное лицо, в том числе:

- наименование или номер социального страхования, дата рождения, номер лицензии или идентификационного номера водителя, регистрационный номер иностранца, номер паспорта работодателя или идентификационный номер налогоплательщика;
- уникальные биометрические данные, такие как отпечатки пальцев, голосовой печати, сетчатки или изображения, и т.д.
- уникальный электронный идентификационный номер, адрес, или код маршрутизации; или

[282] http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm
[283] http://www.ucdmc.ucdavis.edu/compliance/guidance/privacy/deident.html

- уникальная идентифицирующая информация телекоммуникационных устройств или устройства доступа.

В системе национальной безопасности **Privacy policy guidance memorandum: 2007-1 (January 19, 2007)**[284], определяет персональную идентифицирующую информацию как совокупность информации, позволяющей установить идентичность личности, независимо от того, физическое лицо является гражданином Соединенных Штатов, юридические постоянным жителем или посетитель в Соединенных Штатах.

Примеры включают в себя: имя, дату рождения, почтовый адрес, номер телефона, номер социального страхования (SSN), адрес электронной почты, почтовый индекс, номера счетов, номера свидетельств или лицензий, идентификаторы транспортного средства, URL, адреса протокола Интернет, биометрические идентификаторы, фотографические изображения лица или любой другой уникальный идентификационный номер или характеристику или любой другой личной информации.

Таким образом, законодательство США определяет, в общем случае, персональные данные как коммерчески значимую информацию, обладание и законное распространение которой может позволить получить выгоду или избежать ущерба. Получение, хранение, обработка или обращение персональных данных в США регулируется законом именно с точки зрения коммерческой значимости указанной категории информации, что, в свою очередь, порождает понятие cookies, SPAM, Zomby-Net, персонализированную рекламу и т.д.

Таким образом, прослеживается различие между правовыми механизмами обеспечения неприкосновенности частной жизни лица и защитой персональных данных в Российской Федерации:

- в основе правого обеспечения безопасности частной жизни, личной и семейной тайны, защиты чести и доброго имени лежат конституционные принципы, напрямую соотносящиеся с положениями международных актов о правах человека. В то же время в основе защиты персональных данных положены обязательства Российской Федерации в части соблюдения соглашения с Евросоюзом;

[284] Privacy policy guidance memorandum: 2007-1 (January 19, 2007) // http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf

- система правого обеспечения безопасности частной жизни, личной и семейной тайны базируется на строившемся в течение длительного времени комплексе правовых норм, включающих в себя нормы конституционного, гражданского и уголовного права. Система правовых норм в сфере безопасности персональных данных базируется на рекомендациях Евросоюза, причем представляется обоснованным тезис о том, что во многих странах Евросоюза отсутствует практика обеспечения безопасности частной жизни лица, а понятие «персональных данных» нехарактерно для правовой системы США;

- к совокупности информации ограниченного доступа, составляющей содержание частной жизни лица, его личную и семейную тайну, вплотную примыкают сведения, составляющие различные профессиональные тайны, каждая из которых имеет собственный правовой режим, что обеспечивает безопасность различных «сегментов» указанной информации. Понятие персональных данных крайне расплывчато и аморфно, что затрудняет построение правовой системы их защиты;

- правовой режим обеспечения безопасности частной жизни, личной и семейной тайны определяет сведения, порядок доступа и представления, субъектов и ответственность. Безопасность персональных данных в первую очередь определяет требования к информационным технологиям и затрагивает процедурные вопросы (получение согласия, классификация информационных систем и т.д.);

- обеспечение безопасности частной жизни, личной и семейной тайны базируется на нормах общественной морали, в то время, как в социуме отсутствует осознанная необходимость обеспечения защиты персональных данных, подменяемая формальным подходом к получению согласия на обработку персональных данных;

- обеспечение безопасности персональных данных в странах Евросоюза представляет собой новый правовой институт, насчитывающий полтора десятилетия и уже сейчас вступающий в конфликт с правовыми нормами США, протоколами передачи данных в информационных системах и т.д.

3.2. Электронный документ в России и США

Возможность информации свободно передаваться среди участников информационных отношений порождает, с одной стороны, ряд свойств информации, на которые указывалось ранее, с другой стороны, необходимость придания информации некоторой степени организованности, позволяющей учитывать, определять, идентифицировать и совершать в отношении информации иные упорядоченные действия. В связи с этим, вполне обоснованным становиться включение в законодательство понятия «документ», под которым понимается материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения[285].

При этом под документированной информацией понимается зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель[286];

Результатом документирования информации выступает ряд четко выраженных правовых последствий, к числу которых можно отнести:

- выраженную предметную форму документированной информации, позволяющую реализовать право собственности и иные вещные права на материальные носители, содержащие документированную информацию;
- возможность совершения упорядоченных действий в отношении документированной информации,- по восприятию, использованию информации, передаче и предоставлению информации в ходе взаимодействия различных подсистем при хранении, переработке и добыче информации[287];

---

[285] Ст. 1 Федерального закона «Об обязательном экземпляре документов» // СЗ РФ, 02.01.1995, № 1, ст. 1
[286] Ст. 2 Закона об информации
[287] Баранов А.П. Мобильный электронный офис (МЭО) на основе криптографических технологий» // VI-я Международная конференция в сфере электронной торговли

- наличие определенных правил организации документооборота, создания, предоставления, хранения и учета носителей информации[288];
- наибольшую результативность правовых, организационных и технических мер охраны, направленных на обеспечение защиты информации;
- возможность формулировки требований к составу реквизитов документов и бланкам документов;
- наличие требований к характеристикам систем управления документами, включающим в себя надежность, целостность, комплексность и системность.

По физической природе носителя представляется возможным классифицировать документированную информацию как информацию на классическом материальном носителе, атрибутом которой выступает возможность восприятия указанной информации без специальных технических средств; и документированную информацию в виде электронного документа.

В настоящее время в нормативных актах получают широкое распространение понятий «электронного документооборота» и «электронного документа». Некоторыми специалистами высказывается мнение о том, что правовое регулирование электронного документа осуществляется в полном объеме значительным количеством нормативных актов. Действительно, выборка дает более тысячи нормативных актов, так или иначе связанных с электронным документооборотом[289].

При этом основное внимание обращают на Федеральный закон № 63-Ф, определивший под электронной подписью информацию в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Закон представляет собой нормативный акт, устанавливающий только один вид электронной подписи, выработанный на основе ассиметричного криптографического преобразования. Возможности применения других аналогов собственноручной подписи в нем не предусматривается. Закон

[288] Постановление Правительства РФ от 28.07.2005 № 452 «О Типовом регламенте внутренней организации федеральных органов исполнительной власти» // СЗ РФ, 01.08.2005, № 31, ст. 3233; Постановление Правительства РФ от 19.01.2005 № 30 «О Типовом регламенте взаимодействия федеральных органов исполнительной власти» // СЗ РФ, 24.01.2005, № 4, ст. 305

[289] СПС Консультант плюс

закрепляет достаточно сложную процедуру использования электронно-цифровой подписи, подробно регламентирует порядок подтверждения подлинности электронной подписи в открытых и корпоративных информационных системах. Так, если электронная подпись и текст документа принимается как таковой, то открытый ключ электронной подписи подлежит подтверждению: либо стороны на основе дополнительного соглашения принимают его как подлинный, либо используют третью независимую сторону (удостоверяющий центр), которая под свою ответственность подтверждает принадлежность открытого ключа конкретному лицу путем выдачи сертификата.

Таким образом, под электронным документом в смысле этого закона понимается информация в форме, пригодной для обработки, хранения и передачи с использованием электронных средств связи.

В современном виде понятие электронной подписи идентично понятию, заложенному в Типовой закон ЮНСИТРАЛ «Об электронных подписях»[290].

Нормами Закона «Об электронной подписи» ЮНСИТРАЛ определены условия, когда подпись под документом может быть признана юридически значимой:

- данные, представляющие собой электронную подпись, должны быть непосредственно связаны с лицом, подписавшим документ;
- подписание в тот момент, когда оно совершалось, было подконтрольно только подписывавшему лицу;
-легкость выявления изменений электронной подписи, сделанных после подписания;
- легкость выявления изменений в электронном документе.

Кроме того, указанный Закон ЮНСИТРАЛ «Об электронной подписи» содержит указание о том, что законодательство страны может признать надежной ту или иную технологию подписания. Этим будет установлена презумпция, что все документы, подписанные с использованием этой технологии, будут иметь юридическую силу.

[290] Типовой Закон ЮНСИТРАЛ об электронных подписях. Принят в Вене 05.07.2001 на 34-ой сессии ЮНСИТРАЛ // Комиссия ООН по праву международной торговли. Ежегодник. 1996 год. Т. XXVII. Нью-Йорк: Организация Объединенных Наций, 1998. С. 319 - 323.

Указанные положения развиты в Модельном законе «Об электронной цифровой подписи», принятом в г. Санкт-Петербурге 09.12.2000 года Постановлением 16-10 на 16-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ[291].

Особенностью российского Закона № 63-ФЗ «Об электронной подписи»[292]выступает то обстоятельство, что Закон различает простую и усиленную электронную подпись. Усиленная подразделяется на неквалифицированную и квалифицированную. При этом основной акцент сделан не на признании равнозначности электронного документа и документа на бумажном носителе, а на определении условий равнозначности электронного документа (только подписанного электронной подписью) документу на бумажном носителе[293].

Таким образом, закреплен окончательный отказ от введение в правовое пространство сделки в электронной форме как третьей формы сделок, наряду с устной и письменной формами. Законом определено, что при лишь наличии определенных критериев электронной подписи, электронный документ с такой подписью признается равнозначным документу на бумажном носителе с собственноручной подписью.

Информация, подписанная усиленной квалифицированной электронной подписью, признается равнозначной документу на бумажном носителе, за исключением случая, когда федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

Информация, подписанная усиленной неквалифицированной электронной подписью, признается равнозначной в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия, предусматривающими порядок проверки электронной подписи.

К недостаткам такого подхода можно отнести:

---

[291] Модельный закон «Об электронной цифровой подписи». Межпарламентская Ассамблея государств - участников Содружества Независимых Государств // Информационный бюллетень. 2001. N 26. С. 310 - 326.

[292][292] ФЗ «Об электронной подписи» № 63-Ф // РГ. № 75(5451). 8 апреля 2011 г.

[293] Ст. 6 ФЗ "Об электронной подписи" № 63-ФЗ от 6 апреля 2011 г.

- нормативными правовыми актами или соглашением между участниками электронного взаимодействия надлежит предусмотреть правила определения лица, подписывающего электронный документ, по его простой электронной подписи и обязанность лица, создающего и (или) использующего ключ простой электронной подписи, соблюдать его конфиденциальность;

- обязанностью оператора информационной системы надлежит установить правила применения ключа простой электронной подписи;

- существует невозможность формальной ссылки на электронный документ, а лишь на равнозначность документу на бумажном носителе при соблюдении определенных условий.

- указанное обстоятельство является значительной уступкой ряду участников делового оборота, полагающих, что электронными документами являются только лишь текстовые документы, «изготовленные с помощью ЭВМ»[294].

Согласно общепринятой точке зрения, в качестве электронного документа в первую очередь рассматриваются файлы, содержащие тестовую, графическую, аудиовизуальную информацию. Указанная точка зрения является не совсем верной, поскольку значительное количество информации электронно – вычислительной машины содержится именно за пределами содержимого файлов.

По всей видимости, стремление указанное общепринятое заблуждение вытекает из того обстоятельства, что пользователи электронно-вычислительных машин в большинстве своем осуществляют свою деятельность в специально созданных и адаптированных для их удобства интерфейсах, разработанных для использования лицами без специальной подготовки. Использующаяся в указанных пользовательских системах демонстрация процесса ввода и обработки информации в ЭВМ (намеренно, изначально, еще на стадии разработки такой системы) максимально

[294] По поводу термина "документы, изготавливаемые с помощью ЭВМ" см., например: п. 6.1 Единой системы конструкторской документации. Основные надписи. ГОСТ 2.104-2006 (введен Приказом Ростехрегулирования от 22.06.2006 № 118-ст). М.: Стандартинформ, 2006; Ковалева К.Н., Холодная Е.В. Комментарий к Федеральному закону от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (постатейный). М.: Юстицинформ, 2007; Комментарий к Гражданскому кодексу Российской Федерации: В 3 т. Т. 1; Комментарий к Гражданскому кодексу Российской Федерации, части первой (постатейный). 3-е издание, переработанное и дополненное / Под ред. Т.Е. Абовой, А.Ю. Кабалкина. М.: Юрайт-Издат, 2007.

приближена к совершению указанных действий в отношении документов на бумажном носителе. Например, при работе с текстовым документом, пользователь, обладая рядом навыков, осуществляет набор текста почти как на пишущей машинке, текст отображается (обратите внимание) на экране монитора как на листе бумаги. При этом отсутствует какая-либо необходимость вникать в сущность процессов, происходящих в ЭВМ.

Однако, согласно п. 11.1. ФЗ "Об информации"[295] электронный документ представляет собой документированную информацию, представленную в электронной форме, т.е. в виде, пригодном:

- для восприятия человеком с использованием электронно-вычислительных машин;
- для передачи по информационно-телекоммуникационным сетям;
- для обработки в информационных системах.

Информация в электронной (электронно-цифровой) форме представляет собой совокупность электрических импульсов, передаваемых по проводам (каналам связи) либо обрабатываемых процессорами ЭВМ. Электрические импульсы образуются в соответствии с алгоритмом, который, в свою очередь, создается при перекодировании информации в бинарном коде. ЭВМ имеет максимально адаптированные для пользователя устройства ввода и вывода информации (клавиатуру, монитор, динамики и т.д.), однако обработке в ЭВМ подвергаются исключительно электрические импульсы (сигналы). Собственно, именно указанные множества электрических импульсов (сигналов) и являются электронным документом.

При этом следует иметь в виду, что электронный документ как компьютерная информация может быть представлен на нескольких уровнях: физическом (на материальном носителе и находящаяся в процессе взаимодействия с носителем); логическом; синтаксическом; семантическом; прагматическом[296].

Информация на физическом уровне и образует основные, первичные «следы», т.е. материальные отображения внешних признаков предметов.

---

[295] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ, 31.07.2006, № 31 (1 ч.), ст. 3448,

[296] Дуленко В.А. О доказательной ценности компьютерной информации // Правовые вопросы связи, 2006, № 2

На логическом уровне компьютерная информация представлена в виде условных единиц хранения информации различной величины и сложности: байты, блоки, сектора, кластеры, файлы, папки (каталоги), логические или сетевые диски. При этом файл является основным хранителем информации, определяя не только содержание программ и данных, но и их форму и свойства.

На синтаксическом уровне представления компьютерная информация предстает в виде совокупности символов, слов и предложений, используя при этом многие десятки кодировок.

Отдельно следует выделять: системную информацию, информацию в операционной системе, «технологический мусор».

К системной информации относится системный реестр, файлы инициализации, файлы "истории", журналы аудита и др.

Операционная система содержит, например: список недавно запускаемых программ; список документов, с которыми работал каждый из зарегистрированных пользователей; перечень ключевых слов для поиска файлов; адреса посещенных интернет-сайтов и т.д.

Под «технологическим мусором» можно понимать остаточную информацию, создаваемую программным обеспечением для работы режима виртуальной памяти, кэширования, "теневой" памяти, резервирования документов для удобства пользователя.

Определенная часть компьютерной информации может быть защищена криптографическим способом, и, при отсутствии криптографических ключей, доступ к указанной информации фактически невозможен. Современные криптоалгоритмы можно вскрыть либо с помощью очень высококвалифицированных криптоаналитиков и ресурсов суперкомпьютеров, либо путем обычного перебора (не менее чем за несколько десятков лет).

Помимо информации в ЭВМ активно применяются технологии размещения информации в сети ЭВМ. Так, при применении облачных технологий, в общем случае, угрозы информационной безопасности возникают на уровне аппаратных компонентов центров обработки данных, телекоммуникационных составляющих доступа к ресурсам центров обработки данных, программно-аппаратного обеспечения пользователей,

«среднего» (middleware) слоя центра обработки данных (обеспечивающего виртуализацию вычислений и включающего систему управления), прикладных сервисов и систем хранения данных[297].

В том, что касается «документов, изготовленных с помощью ЭВМ», следует иметь в виду, что Инструктивными указаниями Госарбитража СССР от 29 июня 1979 г. «Об использовании в качестве доказательств по арбитражным делам документов, подготовленных с помощью электронно-вычислительной техники», определена возможность сторон по арбитражным делам в обоснование своих требований и возражений представлять документы, подготовленные с помощью электронно-вычислительной техники. Эти документы, поскольку они содержат данные об обстоятельствах, имеющих значение для дела, должны приниматься органами арбитража на общих основаниях в качестве письменных доказательств[298].

Государственный стандарт Союза ССР[299] установил требования к составу и содержанию реквизитов, придающих юридическую силу документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники, а также порядок внесения изменений в эти документы. Стандарт является обязательным для всех предприятий, организаций и учреждений, осуществляющих информационный обмен документами на машинном носителе и машинограммами. Стандарт определял перечень обязательных реквизитов документа на машинном носителе: наименование организации - создателя документа; местонахождение организации - создателя документа или почтовый адрес; наименование документа; дату изготовления документа; код лица, ответственного за правильность изготовления документа на машинном носителе или машинограммы, или, как правило, код лица, утвердившего документ.

Подлинником документа на машинном носителе определялась первая по времени запись документа на машинном носителе и содержащая указание,

[297] Баранов А.П. Можно ли защитить в «облаке» конфиденциальную информацию // Системы высокой доступности, № 2, т. 8, 2012, С. 12

[298] Государственный арбитраж СССР. Инструктивные указания от 29 июня 1979 г. № И-1-4 "Об использовании в качестве доказательств по арбитражным делам документов, подготовленных с помощью электронно-вычислительной техники" // Сборник инструктивных указаний Государственного арбитража СССР. 1983.

[299] ГОСТ 6.10.4-84: «Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники»

что этот документ является подлинником. Дубликатами документа на машинном носителе являются все более поздние по времени, аутентичные по содержанию записи документа на машинном носителе и содержащие указание, что эти документы являются дубликатами. Копиями документа на машинном носителе или машинограмме являются документы, переписанные с подлинника или дубликата документа на машинном носителе или машинограмме на другой носитель информации, аутентичные по содержанию и содержащие указание, что эти документы являются копиями.

ГОСТ 6.10.4-84 впервые закрепил один из основных юридических принципов электронного документооборота: подлинники, дубликаты и копии документа на машинном носителе и машинограммы, полученные стандартными программными средствами вычислительного комплекса, имеют одинаковую юридическую силу, если они оформлены в соответствии с требованиями стандарта.

Документ на машинном носителе и машинограмму следовало применять только при наличии соответствующих решений министерств, ведомств. Документ на машинном носителе и машинограмма приобретали юридическую силу после выполнения требований стандарта и подписания сопроводительного письма.

Гражданский кодекс Российской Федерации (п. 2 ст. 160 ГК РФ), раскрывая письменную форму сделки, определяет, что использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронной подписи либо иного аналога собственноручной подписи допускается в случаях и в порядке, которые предусмотрены законом, иными правовыми актами или соглашением сторон. П. 2 ст. 434 ГК РФ установлено, что договор в письменной форме может быть заключен также и путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору.

Изложенное позволяет сделать вывод, что современный практический подход к электронному документу делает акцент на его составляющей как документированной информации, пригодной для восприятия человеком с использованием электронно-вычислительных машин, оставляя без внимания

ее представление в виде, пригодном для передачи по информационно-телекоммуникационным сетям и для обработки в информационных системах.

Указанная неосведомленность пользователя не имеет существенного значения при заведомой добросовестности участников, при отсутствии конфликтов[300].

При возникновении спора, учитывая необходимость доказывания, используется следующий прием: нотариус устанавливает соответствие между изображением на экране монитора и распечаткой указанного изображения на бумажном носителе (скриншотом), заверяет указанную распечатку, в каком виде она представляется в качестве письменного доказательства.

Постановлением Пленума Верховного Суда СССР от 3 апреля 1987 г. № 3 «О строгом соблюдении процессуального законодательства при осуществлении правосудия по гражданским делам»[301] определялось, что в случае необходимости судом могут быть приняты в качестве письменных доказательств документы, полученные с помощью электронно-вычислительной техники, каковые материалы оцениваются в совокупности с другими доказательствами"[302].

Руководящими разъяснениями п.6 Постановления Пленума Верховного Суда СССР № 7 от 9 июля 1982 г. «О судебном решении» указывается, что в обоснование решения суд в случае необходимости вправе сослаться и на письменные доказательства в виде документов, полученных с помощью электронно - вычислительной техники. Эти документы принимаются в качестве доказательств при условии их надлежащего оформления в соответствии с установленным порядком[303].

Высший арбитражный суд РФ дал оценку доказательств изготовленных и подписанных с помощью средств электронно-вычислительной техники, в которых использована система цифровой (электронной) подписи[304].

---

[300] Жарова А.К. О конфликте интересов субъектов в информационных отношениях // Государство и право. 2011. № 4. С. 42-49.

[301] В настоящее время признано утратившим силу.

[302] Постановление Пленума Верховного Суда СССР от 3 апреля 1987 г. № 3 «О строгом соблюдении процессуального законодательства при осуществлении правосудия по гражданским делам» // Бюллетень Верховного Суда СССР. 1987, № 3.

[303] Постановление Пленума Верховного Суда СССР № 7 от 9 июля 1982 г. "О судебном решении" // Бюллетень Верховного Суда СССР, № 4, 1982

[304] Письмо ВАС РФ от 19 августа 1994 г. № С1-7/ОП-587 "Об отдельных рекомендациях, принятых на совещаниях по судебно-арбитражной практике".

Одновременно, практическое разрешение указанных вопросов сопровождалось бурной научной полемикой о месте электронных документов в системе доказательств. При этом следует выделять две точки зрения:

- современные источники информации охватываются уже известными процессуальному законодательству средствами доказывания и их необходимо относить или к вещественным, или к письменным доказательствам;
- современные источники информации не охватываются уже установленными средствами доказывания, их нельзя относить к вещественным или к письменным доказательствам (документам).

Аргументируя обоснованность первой из них, Д.М. Чечот отмечал, что специфические особенности носителя информации предполагают специфические способы ее воспроизведения, т.е. если документ на обычном носителе может быть воспринят обычным способом (непосредственно прочитан), то «технический носитель информации во многих случаях требует расшифровки»[305]. Указанное обстоятельство, между тем не помешало автору отнести к письменным доказательствам перфокарты, магнитные ленты, перфоленты.

По мнению Е.А. Виноградовой, «действующее гражданское и процессуальное законодательство давало и дает основания для формирования судебной практики, исходящей из принципиальной допустимости в качестве письменных доказательств в суде, в госарбитраже заверенных электронной цифровой подписью документов»[306].

В.Г. Тихиня рассматривал магнитные записи в качестве вещественных доказательств[307].

А.В.Ткачев полагал, что «Целесообразность введения в право нового вида доказательств вызывает большое сомнение, т.к., во-первых, компьютерные документы уже достаточно широко и эффективно применяются в самых различных правоотношениях в качестве документов, во-вторых,

---

[305] Советский гражданский процесс / Под ред. Н.А. Чечиной, Д.М. Чечота. Ленинград, 1984. С. 156.
[306] Виноградова Е. Правовое регулирование создания и использования электронной (безбумажной) документации, заверенной электронной цифровой подписью // Хозяйство и право. 1994. № 5. С. 64 - 66.
[307] Тихиня В.Г. Применение криминалистической тактики в гражданском процессе. Минск, 1976. С. 10 - 11.

законодательное определение документа-доказательства вполне позволяет урегулировать технико-технологические особенности этих документов»[308].

А.П. Вершинин считает, что электронная форма документа усложняет его использование в качестве письменного доказательства в гражданском и арбитражном процессе, так как в отличие от письменных документов электронные документы сами по себе недоступны человеческому восприятию, в связи с чем они имеют большее сходство с вещественными доказательствами, которые служат средством установления обстоятельств, имеющих значение для дела[309].

Как легко видеть, сторонники «традиционалистского подхода» испытывали определенные сложности по вопросу отнесения электронных документов к письменным доказательствам, либо к иным документам.

В обоснование второй точки зрения М.К. Треушников указывал, что современные источники информации не охватываются уже установленными средствами доказывания. Их необходимо считать самостоятельными средствами доказывания, и, соответственно, для допуска их в процесс в качестве средств доказывания необходимо вносить соответствующие изменения в действующее процессуальное законодательство, поскольку «воспроизведение сохраняющейся на магнитных носителях информации требует отличных от письменных и вещественных доказательств методов»[310].

По мнению А.Т. Боннер «машинные документы вряд ли можно автоматически относить к традиционным письменным, а иные современные средства фиксации информации - к вещественным доказательствам, поскольку они, как и иные современные процессуальные средства хранения информации: видеозаписи, фотографии, кинофильмы и т.п., обладают существенной спецификой, которая должна быть отражена как в материальном, так и процессуальном законодательстве.»[311] В связи с изложенным предлагалось выделить в качестве самостоятельных средств доказывания машинные документы, фотографии, киноленты, магнитные и

[308] Ткачев А.В. Правовой статус компьютерных документов: основные характеристики. М.: Городец-издат, 2000. С. 54

[309] Вершинин А.П. Электронный документ: правовая форма и доказательство в суде. М.: 2000. С. 109

[310] Треушников М.К. Судебные доказательства. М., 1999. С. 97.

[311] Боннер А.Т. Правило допустимости доказательств в гражданском процессе: необходимость или анахронизм? // Советское государство и право. 1990. № 10. С. 30.

видеозаписи, а также иные источники, полученные с помощью научно-технических средств.

И.З. Карась отмечает, что новые способы фиксации информации в памяти ЭВМ «позволяют ставить вопрос об обособлении записей в памяти ЭВМ в новый класс информационно-вычислительных доказательств»[312].

Ю.М. Батурин включал электронные документы в отдельный вид «документально-компьютерных доказательств»[313].

По мнению А.Г. Прохорова следует выделить магнитные записи в самостоятельное средство доказывания[314].

Точка в указанном споре была положена принятием Гражданско-процессуального и Арбитражно-процессуального кодексов, которые, хотя и не выделили электронный документ в самостоятельную категорию доказательств, однако указали их точное место в структуре доказательств по гражданским и арбитражным делам.

Так, согласно п. 1 ст. 71 ГПК РФ к письменным доказательствам относятся документы и материалы, выполненные в форме цифровой, графической записи, в том числе полученные посредством факсимильной, электронной или другой связи.

Статья 60 АПК РФ прямо указывает на возможность использования в качестве источников письменных доказательств в арбитражном процессе договоров, справок, деловой корреспонденции, иных документов и материалов, в том числе полученных посредством факсимильной, электронной или иной связи (т.е. электронных документов – авт.).

Требованиями ч. 3 ст. 75 АПК РФ определено, что документы, полученные посредством факсимильной, электронной или иной связи, а также документы, подписанные электронной цифровой подписью или иным аналогом собственноручной подписи, допускаются в качестве письменных доказательств в случаях и в порядке, которые установлены федеральным законом, иным нормативным правовым актом или договором.

---

[312] Карась И.З. Юридические факты и доказательства в информационных правоотношениях // Советское государство и право. 1988. № 11. С. 92

[313] Батурин Ю.М. Проблемы компьютерного права. М.: Юрид. лит., 1991. С. 184.

[314] Прохоров А.Г. Принцип допустимости средств доказывания в советском гражданском процессуальном праве. Автореферат диссертации на соискание ученой степени кандидата юридических наук. Свердловск, 1979.

Следует особо подчеркнуть, что в российском гражданском и арбитражном процессах, особую значимость приобрело не соотнесение электронного документа – документам на бумажном носителе, а выделение электронного документа в самостоятельную категорию доказательств (формально относящихся к письменным доказательствам).

В уголовном процессе ч. 2 ст. 74 УПК РФ определен перечень видов доказательств, который является исчерпывающим и расширительному толкованию не подлежит. К ним относятся показания подозреваемого, обвиняемого, потерпевшего и свидетеля; заключение и показания эксперта; заключение и показания специалиста; вещественные доказательства; протоколы следственных действий и судебного заседания; иные документы, содержащие сведения, относящиеся к уголовному делу.

При этом следует иметь в виду, что согласно легальному определению ст. 81 УПК РФ вещественным доказательством признаются любые предметы:

- которые служили орудиями преступления или сохранили на себе следы преступления;
- на которые были направлены преступные действия;
- деньги, ценности и иное имущество, полученные в результате совершения преступления;
- иные предметы и документы, которые могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела.

Статья 84 УПК РФ определяет, что иные документы допускаются в качестве доказательств, если изложенные в них сведения имеют значение для установления обстоятельств имеющих значение для дела.

Документы могут содержать сведения, зафиксированные как в письменном, так и в ином виде. К ним могут относиться материалы фото- и киносъемки, аудио- и видеозаписи и иные носители информации, полученные, истребованные или представленные в порядке, установленном ст. 86 УПК РФ.

При этом обращает на себя особое внимание явно выраженная «материальная форма» доказательств, могущие быть или предметами (ст.81 УПК РФ), либо сведениями, зафиксированными как в письменном, так и в ином виде (материалы фото- и киносъемки, аудио- и видеозаписи и иные носители информации). В уголовном процессе также используются:

электронная почта, электронные средства контроля поведения, системы видеоконференц-связи, ЭД подписанного судьей усиленной квалифицированной электронной подписью. С декабря 2012 года УПК РФ дополнен нормой п.п. 2.1 ч. 4 ст. ч. 82 УПК РФ (Хранение вещественных доказательств), определяющей порядок производства следственных действий в отношении электронных носителей информации.

Таким образом, Уголовно-процессуальный кодекс РФ напрямую не включает компьютерную информацию в исчерпывающий перечень допустимых доказательств. Использование информационных и компьютерных технологий в качестве доказательств возможно в случае их отнесения к категориям: заключений и показаний экспертов (специалистов), вещественных доказательств или иных документов[315].

Электронный документ может рассматриваться в качестве доказательства по уголовным делам лишь в виде вещественного доказательства, либо в качестве иных документов, относящихся к уголовному делу. Указанная неопределенность осложняет возможности расследования дел, направленных, в первую очередь, на борьбу с преступлениями в сфере компьютерной информации, порождает споры в среде ученых-криминалистов о месте компьютерной информации в системе доказательств (аналогичные спорам ученых – цивилистов по тому же вопросу).

Анализ зарубежного законодательства свидетельствует о том, что в ряде стран электронному документу придается гораздо большее значение, нежели в нашей стране.

Директива ЕС 2001/115/ЕС. об электронных подписях[316] содержит два определения электронной подписи: обычная электронная подпись и специальная (усиленная) электронная подпись. Под электронной подписью в Директиве понимаются "данные в электронной форме, которые приложены либо логически присоединены к иным электронным данным, используемые как метод аутентификации", а под специальной электронной подписью

[315] Elin V. Evidentiary value of electronic documents in the Russian procedural law // Human Rights on the Internet: Legal Frames and Technological Implications: Compendium on Internet Governance. HSE. -M., 2012. -P. 74.

[316] Directive No. 1999/93/EC Of the European Parliament and of The Council On A Community Framework For Electronic Signatures (Brussels, 13.XII.1999). Amended by Regulation (EC) No 1137/2008 of the European Parliament and of the Council of 22 October 2008 // http://eur-lex.europa.eu/

(advanced electronic signature) в Директиве понимается электронная подпись, которая отвечает следующим требованиям:

- относится исключительно к подписывающему лицу;
- позволяет идентифицировать подписывающее лицо;
- создана с помощью средств, которые подписывающее лицо может иметь под своим исключительным контролем;
- соединена с данными, к которым она относится, таким образом, что имеется возможность обнаружить последующую модификацию таких данных.

Ст. 2 Типового закона ЮНСИТРАЛ об электронной торговле, одобренного 16 декабря 1996 г. Резолюцией 51/162 на 85-м пленарном заседании Генеральной Ассамблеи ООН, используется термин "Datamessage" (дословный перевод - "передача данных"), под которым понимается информация, подготовленная, отправленная, полученная или хранимая с помощью электронных, оптических или аналогичных средств, включая электронный обмен данными, электронную почту, телекс или телефакс и т.д. Электронный обмен данными раскрывается как электронная передача информации от компьютера к компьютеру в соответствии с согласованными стандартами структуры информации[317].

Указанная точка зрения поддерживается также и Директивой 2000/31/ЕС Европейского Парламента и Совета от 8 июня 2000 г. о некоторых правовых аспектах услуг информационного общества, и в частности об электронной торговле на внутреннем рынке (Директивой об электронной торговле)[318].

Конвенцией о киберпреступности[319] определено, что страны-участницы принимают законодательные и иные меры, необходимые для установления полномочий и процедур в целях проведения конкретных уголовных расследований или судебного разбирательства в отношении:

---

[317] Комиссия ООН по праву международной торговли. Ежегодник. 1996 год. Т. XXVII. Нью-Йорк: Организация Объединенных Наций, 1998. С. 319 - 323.

[318] Directive No. 2000/31/EC of the European Parliament and of The Council «On Certain Legal Aspects Of Information Society Services, In Particular Electronic Commerce, In The Internal Market (Directive On Electronic Commerce) // http://eur-lex.europa.eu/

[319] Convention On Cybercrime (Budapest, 23.XI.2001). Конвенция о преступности в сфере компьютерной информации (ETS№ 185) заключена в г. Будапеште 23.11.2001. Распоряжением Президента РФ от 15.11.2005 № 557-рп Российская Федерация приняла решение подписать Конвенцию с заявлением об условии возможного пересмотра положений пункта «в» ст. 32 указанной Конвенции. В 2008 г. Распоряжением Президента РФ от 22.03.2008 № 144-рп распоряжение Президента РФ от 15.11.2005 № 557-рп признано утратившим силу.

- уголовных киберпреступлений: против конфиденциальности, целостности и доступности компьютерных данных и систем, связанных с использованием компьютерных средств, содержанием данных и с нарушением авторского и смежного прав;

- других уголовных преступлений, совершенных при помощи компьютерной системы;

- сбора доказательств в электронной форме уголовного преступления.

К указанным мерам совершенствования процессуального законодательства следует относить:

- оперативное обеспечение сохранности хранимых компьютерных данных (ст.16);

- оперативное обеспечение сохранности и частичное раскрытие данных о потоках информации (ст. 17);

- распоряжение о предъявлении (ст.18);

- обыск и выемка хранимых компьютерных данных (ст.19);

- сбор в режиме реального времени данных о потоках информации и перехват данных о содержании (ст.ст.20,21).

В настоящее время наша страна отказалась от участия в данном интеграционном процессе на основании, неприемлемости положения п. «в» ст. 32 Конвенции, в связи с угрозой нанесения [320]ущерба суверенитету и национальной безопасности государств-участников, правам и законным интересам их граждан и юридических лиц.

В США основными источниками американского права, регулирующими использование доказательств, полученных с помощью компьютера, служат принятые Федеральные правила уголовного процесса и Федеральные правила о доказательствах[321]. Кроме того, ряд положений содержится в **USA Patriot Act, Federal Criminal Code Related to Computer Intrusions**, многочисленных судебных прецедентах.

---

[320] Ст. 32: сторона может без согласия другой стороны:

"b"- получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получать их, если эта сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой стороне через такую компьютерную систему.

[321] Federal Criminal Code and Rules. Federal Rules of Criminal Procedure. West Group. St. Paul, Minn. 1997. P. 257, 342, 379. Federal Rules of Evidence for United States Courts and Magistrates // Federal Rules of Evidence, 2004 - 2005 Edition. Also including California Evidence Code (with selected comments), Uniform Rules of Evidence, Westlaw Electronic research guide, Report on caselaw divergence from FRE. West Group; 3d Bk & Map edition, 2004.

Федеральные правила о доказательствах не содержат непосредственного упоминания компьютерных доказательств. Однако комментарии и судебная практика позволяют утверждать, что Правила создавались с расчетом их применения к "нетрадиционным" доказательствам, к которым также относятся электронные документы.

В том, что касается Федеральных правил уголовного процесса, следует иметь в виду, что электронные документы как доказательства подразделяются на прямые (non-hearsay), косвенные (hearsay) и сочетающие в себе свойства тех и других[322].

К прямым доказательствам относят те из них, которые сгенерированы ЭВМ без участия человека и подразделяются на две категории:

- computer-generated records (записи, созданные компьютером);

- computer-stored records (записи, хранящиеся в памяти ЭВМ).

Существует также достаточно обоснованная точка зрения о выделении третьей категории, включающей в себя сочетание двух вышеназванных[323].

Hearsay содержат результат деятельности людей (личные письма, памятки, документы бухгалтерского учета и т.д.), созданные людьми, но никак не журналы или записи компьютерных процессов, к которым применяются правила исследования косвенных доказательств. Некоторые компьютерные данные полностью отвечают требованиям hearsay.

По происхождению различают две основные группы компьютерных доказательств[324]:

- результат деятельности человека, сохраненный на электронном носителе (computer-stored evidence, human generated computer evidence), т.е. данные, хранящиеся на электронных носителях (жестком диске, флоппи-диске, компакт-диске, стримере) и содержащие информацию, внесенную пользователем;

- доказательство, созданное компьютером в соответствии с заложенной программой, являющееся производным от доказательств первого вида и

[322] Searching and obtaining electronic evidence Manual. Chapter 3 // United States Department of Justice // cybercrime.Gov/ssmanual/05ssma.html.
[323] Orin S. Kerr Computer Records and Federal Rules of Evidence // United States Department of Justice // cybercrime.Gov/http://content.hccfl.edu/pollock/aunix2/KerrComputerRecords.pdf.
[324] Иванов Н. Допустимость компьютерных доказательств в процессуальном праве России и США // Адвокат. 2000. № 5.

представляющее собой результат обработки тех или иных начальных данных в соответствии с заложенной в компьютер программой.

Классификация по сущности доказательства подразделяется на доказательства:

- созданные человеком в ЭВМ (human generated computer evidence);

- созданные компьютером (computer-stored evidence);

- созданные совместно человеком и компьютером.

По форме доказательства подразделяют на:

- raw data (исходные данные), включающие данные, введенные человеком и относящиеся к документам в целом;

- databases (базы данных);

- codes necessary to interpret computer information (коды, необходимые для расшифровки электронной информации);

- commercial software (программное обеспечение коммерческого характера);

- computer systems (компьютерные системы), под которыми понимаются ЭВМ, серверы, локальные сети, магнитные носители различных видов.

Классификация по форме представления определяется тем обстоятельством, что существуют два возможных формата электронной информации: hard copy (твердая или жесткая копия) и machine readable format (машиночитаемая копия).

При этом определен ряд требований к электронному документу как процессуальному доказательству.

Перед принятием электронного документа в качестве доказательства участник процесса должен доказать его аутентичность (show that it is authentic), что возможно следующими способами:

- при помощи стандартной процедуры аутентификации электронного документа, как и любой другой записи, в соответствии с неполным списком Федеральных правил доказывания[325];

- для демонстрации аутентификации записей, сгенерированных компьютером, сторона должна представить описание процесса или систему, используемую для получения результата, и показать, что процесс или система производят точный результат. В большинстве случаев надежность

[325] Federal Rule of Evidence. Art. 901 (b).

компьютерной программы устанавливается на основании ее использования значительным числом пользователей на постоянной основе;

- когда компьютерная программа не используется на регулярной основе, сторона обязана раскрыть, какие операции компьютеру было поручено выполнять, а также точные инструкции, которые были даны ЭВМ.

При этом разрешаются два вопроса:

- установление подлинности (evidence sufficient to support afinding that the matter in questions is what its proponent claims);

- установление достоверности (not inadmissible hearsay).

Раскрывая подлинность записей ЭВМ, законодательство США основывается на:

- постулате, что в отсутствие конкретных доказательств того, что произошло вмешательство, сама возможность вмешательства не влияет на достоверность компьютерной записи (Absent specific evidence that tampering occurred, the merepossibility of tampering does not affect the authenticity of computerrecord);

- правиле лучшего доказательства, не требующем представления оригинала записи в суд[326];

- ограничениях представления в суд "сборников" компьютерных распечаток, основанных на Правиле 1006[327].

В части электронного документа как косвенного доказательства действуют следующие положения:

- неприменение правил о косвенных доказательствах к электронным документам, сгенерированным ЭВМ;

- применение правил о косвенных доказательствах в отношении записей, хранящихся в ЭВМ.

Положения Федеральных правил о доказательствах[328] требуют представления информации в пригодном для использования виде. Во многих случаях таковой признается жесткая копия - распечатка содержимого файла на бумаге. Однако правило не содержит положений, запрещающих или ограничивающих использование второго формата. Ряд прецедентов устанавливает, что при определенных обстоятельствах жесткая копия не

[326] Federal Rules of Evidence. Art. 1002.
[327] Federal Rules of Evidence. Art. 1006.
[328] Federal Rules of Evidence. Art. 34.

может признаваться "пригодной для использования" и предписывает стороне предоставить данные в машиночитаемом формате - в виде перфокарт, магнитных лент, дискет, компакт-дисков, zipp-дисков или непосредственно жестких дисков компьютера.

Как следует из вышесказанного, вопросам использования электронного документа в качестве доказательства по уголовным делам в США уделяется значительное внимание. Возникает обоснованный вопрос об исключительности США, возможности применения их опыта на современной нам технической базе и уровне компьютерной грамотности и т.д.

Применяя сложившееся в процессе отношение к электронному документу как доказательству, следует с горечью констатировать, что наша страна к участию в интеграционных процессах не готова и готова не будет по крайней мере до тех пор, пока в общественном сознании электронный документ не будет представляться чем-то большим, нежели "документом, изготовленным с помощью ЭВМ".

Однако следует уделять значительное внимание вопросам применения электронного документа, хотя бы потому, что в силу трансграничности передачи компьютерных данных наши российские граждане и юридические лица становятся субъектами международного информационного обмена.

Таким образом, возможность использования электронного документа в качестве доказательства осложняется существованием ряда проблем:

- в настоящее время определены условия только лишь равнозначности электронного документа (только подписанного электронной подписью) и документа на бумажном носителе при отсутствии собственно равенства между электронным документом и документом на бумажном носителе;

- при использовании электронного документа в качестве доказательства по уголовным делам основной акцент делается на материальную составляющую информационного объекта, но никак не на информационную компоненту его;

- не определены место и роль электронного документа в качестве доказательства по уголовным делам;

- не предпринимаются меры по интеграции подходов в данном вопросе с существующими международными соглашениями и практическими наработками в данной сфере в других государствах.

Устранение указанных проблем можно осуществить как внесением изменений в отраслевое законодательство, так и путем скорейшего принятия Информационного кодекса РФ либо Закона «Об электронном документе».