ПРАВО ПОЛЬЗОВАТЕЛЕЙ УСЛУГ ПЕРЕДАЧИ ДАННЫХ НА ТАЙНУ СООБЩЕНИЙ

Авторы[254]***:***

Миськевич А.Ю., *старший преподаватель кафедры теории и истории государства и права Гродненского государственного университета имени Янки Купалы;*

Седельник В.В., *заведующая кафедрой теории и истории государства и права Гродненского государственного университета имени Янки Купалы, кандидат юридических наук, доцент;*

Просвирнина И.Б., *доцент кафедры математического анализа, дифференциальных уравнений и алгебры Гродненского государственного университета имени Янки Купалы, кандидат физико-математических наук, доцент;*

Кацубо С.П., *заведующая кафедрой социально-гуманитарных и правовых дисциплин Гомельского государственного технического университета имени П.О. Сухого, кандидат юридических наук, доцент.*

Введение

Несмотря на общепринятую четырехзвенную концепцию защиты информационной безопасности: технические, программные, организационные и правовые меры, существенно отличаются подходы IT-специалистов и юристов по защите тайны сообщений. IT-специалисты рассматривают защиту информационных ресурсов, систем и сетей. Юристы рассматривают защищенность прав и интересов в информационной сфере. Для юриста при анализе информационных отношений сложно определить места субъектов в структуре правоотношения. С технической точки зрения сложно объяснить, что любой процесс обработки информации — это правоотношение. Для более эффективной защиты права на тайну сообщений необходима гармонизация технического и юридического подходов. Начать следовало бы с выработки общей теории, из которой бы исходили как представители точных, так и гуманитарных наук при решении проблем, связанных с защитой информации.

Законодательство Республики Беларусь, регулирующее отношения по передаче, предоставлению и распространению информации, несмотря на относительно большое количество принятых нормативных актов, все еще находится на стадии становления. Некоторые нормативные правовые акты, очевидно, нуждаются в дополнениях. При разработке таких дополнений наблюдается тенденция трактовки информационной безопасности только как составной части национальной безопасности, то есть

[254] *Коллектив авторов выражает благодарность за помощь в подготовке исследования студенту Белорусского государственного экономического университета Кравцову Павлу.*

как раз такого блага, которое часто применяется как причина для ограничения прав человека. Такая тенденция должна быть компенсирована правовыми исследованиями в области информационной безопасности с точки зрения человека и во имя его прав.

Необходимо выявить ситуации, в которых право человека на тайну сообщений формально защищено, однако правовой защитой по разным причинам человек не может воспользоваться. Согласно социологическим данным, «только 13 % пользователей считают, что белорусское законодательство гарантирует право на анонимность и защиту от произвольного надзора / слежки за коммуникацией онлайн. Только 25 % пользователей считают, что белорусское законодательство гарантирует защиту персональных данных»[255]. Необходимо выявить, что останавливает человека перед тем, чтобы добиваться защиты своего права: несовершенство механизма защиты права или простое безразличие. «Только 45 % респондентов отдают предпочтение неприкосновенности частной жизни перед удобством электронных сервисов»[256]. Также необходимо выявить ситуации, в которых право пользователей услуг передачи данных на тайну сообщений даже формально не защищается. Растет число пользователей, которые лично сталкивались с нарушением права на защиту персональных данных. В 2019 г. таких пользователей оказалось «34 % против 22 % в 2015 г.»[257].

Правовое исследование, претендующее на то, чтобы ответить на такие вопросы должно сопровождаться учетом, разъяснением основ и деталей технологий работы с компьютерной информацией, в частности технологии создания, передачи и получения сообщений с помощью компьютерных программ.

Цель исследования: определить механизм правовой защиты права на тайну сообщений пользователей услуг передачи данных и разработать рекомендации и предложения по его совершенствованию.

Задачи исследования

1. Разработка междисциплинарного концептуального аппарата в области защиты права на тайну сообщений пользователей услуг передачи данных.

2. Анализ норм международного права в области защиты права на тайну сообщений пользователей услуг передачи данных от киберправонарушителей.

---

[255] *Онлайновый активизм и цифровые свободы: Беларусь 2019 [Электронный ресурс] : Исследование: онлайновый активизм и цифровые права // Human Constanta. Режим доступа : https://humanconstanta.by/wp-content/uploads/2019/04/HumanConstanta_Presentation_29.03.19.pdf. Дата доступа : 05.09.2019.*

[256] *Там же.*

[257] *Онлайновый активизм и цифровые свободы: Беларусь 2019 [Электронный ресурс] : Исследование: онлайновый активизм и цифровые права // Human Constanta. Режим доступа : https://humanconstanta.by/wp-content/uploads/2019/04/HumanConstanta_Presentation_29.03.19.pdf. Дата доступа : 05.09.2019.*

3. Характеристика комплекса правовых норм Республики Беларусь о тайне сообщений пользователей услуг передачи данных и выявление дефектов в правовой регламентации данного права.

4. Исследование совместимости правовых и криптографических мер защиты тайны сообщений пользователей услуг передачи данных .

5. Анализ правового механизма защиты тайны сообщений пользователей услуг передачи данных от киберправонарушителей.

6. Определение перспектив совершенствования механизма защиты тайны сообщений пользователей услуг передачи данных от киберправонарушителей.

Объект исследования: право на тайну сообщений пользователей услуг передачи данных.

Предмет исследования: правовой механизм защиты тайны сообщений пользователей услуг передачи данных (ПУПД).

Гипотеза исследования

Действующие нормы о праве на тайну сообщений ПУПД должны быть дополнены. Те способы защиты данного права, которые существуют, являются недостаточно эффективными. Существует ряд факторов, которые препятствуют человеку защитить его право на тайну сообщений ПУПД.

Гендерно нейтральный характер исследования

При анализе правового механизма защиты права на тайну сообщений авторы предприняли попытку выявить отличия в проблемах защиты данного права для различных гендерных групп. В ходе исследования таких отличий выявлено не было. Бенефициаром права на тайну сообщений пользователей услуг передачи данных является практически любой человек. В силу этого в теме исследования не усматривается гендерный аспект.

Методология исследования

Специфика данного исследования обуславливается существующей до сих пор значительной разницей в техническом и правовом подходах к защите тайны сообщений. Технические и программные меры по защите права на тайну сообщений — это всего лишь работа над ошибками. Технические меры могут лишь совершенствоваться в результате выявления новых угроз конфиденциальности и приватности информации, но не могут восстановить уже утраченную конфиденциальность и приватность. Правовые же меры представляют собой как механизмы защиты права до его нарушения, так и механизмы восстановления права после его нарушения. Нами была поставлена такая задача, чтобы применение правовых мер защиты права на тайну сообщений шло неотрывно от технических и программных мер защиты.

В исследовании применялись как традиционно правовые методы, так и традиционные методы информатики, а также общие для обеих наук междисциплинарные методы:

- общенаучные методы — анализ, синтез, классификация, абстрагирование, сравнение;

- специальные методы — семиотический, социологический, статистический;
- частные юридические методы и методы информатики — формально-юридический, сравнительно-правовой, метод правового моделирования, метод виртуализации, метод концептуальной трансдукции.

6.1. Понятийные и структурные аспекты правового механизма защиты права на тайну сообщений пользователей услуг передачи данных

Состояние научных исследований по данной теме

На современном этапе развития новейшие цифровые технологии широко используются в мировой системе коммуникаций, что предъявляет определенные требования к защите личных данных и частной жизни пользователя. Научные взгляды на вопросы защиты тайны сообщений развились из концепций защиты права на неприкосновенность частной жизни. Значительное внимание вопросам тайны частной жизни стало уделяться после принятия Всеобщей декларации прав человека в 1948 г., которая распространила понятие неприкосновенности частной жизни на тайну корреспонденции.

В Беларуси правовые и социальные вопросы развития информационного общества и некоторые вопросы защиты персональных данных исследуют Н.А. Антонович, М.С. Абламейко, В.В. Анищенко, Е.М. Бабосов, Г.А. Василевич, А.В. Гусев, А.Н. Данилов, С.В. Енин, А.И. Жук, Е.М. Ильина, С.Н. Князев, А.Н. Курбацкий, О.Н. Мороз, Б.Н. Паньшин, Ю.В. Пономаренко, С.В. Решетников, А.К. Сутурин, Т.З. Шалаева и др.

Проблемы функционирования системы обеспечения информационной безопасности с точки зрения технических наук нашли отражение в трудах А.Л. Балыбердина, М.А. Вуса, В.А. Герасименко, А.А. Грушо, С.В. Дворянкина, П.Д. Зегжды, Е.В. Касперского, В.Д. Курушина, А.А. Малюка, В.А. Минаева, В.Е. Потанина, В.Н. Саблина, С.В. Скрыля, А.П. Фисуна и ряда других ученых.

Некоторые аспекты защиты тайны сообщений рассматриваются также в публикациях технических специалистов. Так, В.П. Дьяконов в своей работе описывает правила эксплуатации, стандарты и рекомендации по применению электронных устройств связи[258]. Практические аспекты предоставления прав на использование компьютерных программ (программных продуктов) в Республике Беларусь освещались М.В. Нехай[259].

---

[258] *Дьяконов, В.П. Электронные средства связи / В.П. Дьяконов, А.А. Образцов, В.Ю. Смердов. М. : СОЛОН-ПРЕСС, 2009. 430 с.*

[259] *Нехай, М.В. Практические аспекты предоставления прав на использование компьютерных программ (программных продуктов) в Республике Беларусь [Электронный ресурс] / М.В. Нехай // КонсультантПлюс, 2019.*

Следует отметить, что комплексного научного исследования по вопросам защиты права на тайну сообщений пользователей услуг передачи данных не проводилось.

Остановимся на некоторых научных публикациях, представляющих, на наш взгляд, интерес при исследовании правого регулирования и защиты права на тайну сообщений.

В некоторой мере отдельные аспекты защиты персональных данных рассматривались в диссертационном исследовании Просветовой О.Б., которое посвящено анализу правовых аспектов, обеспечивающих защиту конфиденциальной информации персонального характера. Автором сформулированы определения таких категорий, как «персональные данные», «информационные процессы», «автоматическая обработка персональных данных», «распространение сведений», разработан перечень категорий сведений, относимых к конфиденциальной информации о гражданах (персональным данным)[260].

Ряд российских исследователей обозначают проблемы защиты персональных данных работников[261], угрозы персональным данным пользователей в системах дистанционного обучения образовательных организаций[262], современные проблемы информационной безопасности личности [263].

Представляет интерес работа украинского автора, профессора Кохановской Е.В. об осуществлении и защите прав физических лиц в информационной сфере гражданского общества[264]. Автор, рассматривая защиту информационных отношений существенной составляющей информационной безопасности, считает важным говорить о защите именно информационных отношений, а не только о защите информационных прав, поскольку защите подлежат как объекты этих отношений, так и субъекты, а не только их права.

В рамках анализа норм международных правовых актов, регулирующих отношения по предмету исследования, авторами проанализирован ряд научных публикаций Довгань Е.Ф.[265], в которых затрагиваются про-

---

[260] *Просветова, О.Б. Защита персональных данных: автореф. дис. … канд. юрид. наук: 05.13.19 / О.Б. Просветова ; Воронежский институт МВД России. Воронеж, 2005. 24 с.*

[261] *Меньшикова, А.В. Некоторые проблемы защиты персональных данных работника, перспективы и пути их решения [Электронный ресурс] / А.В. Меньшикова // Экономика и менеджмент инновационных технологий. Режим доступа : http://ekonomika.snauka.ru/2014/11/6440. Дата доступа : 05.09.2019.*

[262] *Шугай, А.А. Защита персональных данных: международный опыт правового регулирования / А.А. Шугай // Пром.-торг. Право. 2015. №3. С. 87—91.*

[263] *Никитин, П.В., Капелькина, А.В., Фархшатов, И.В. Современные проблемы информационной безопасности личности [Электронный ресурс] / П.В. Никитин, А.В. Капелькина, И. В. Фархшатов // Международный студенческий научный вестник. Режим доступа : http://eduherald.ru/ru/article/view?id=14280. Дата доступа : 24.09.2019.*

[264] *Кохановская, Е.В. Осуществление и защита прав физических лиц в информационной сфере гражданского общества Е.В. Кохановская // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019.*

[265] *Довгань, Е.Ф. Правомерность целевых санкций Совета Безопасности ООН в рамках борьбы с терроризмом / Е.Ф. Довгань // Научно-практический журнал «Право.by». 2011. № 3. С. 11—20.*

блемы статуса международных организаций, рассматриваются основные группы принимаемых ими актов и их правовая сила.

Абламейко М.С., Василевич Г.А. с целью реализации основных направлений, определенных в Стратегии развития информационного общества в Республике Беларусь, обосновывают разработку информационного кодекса, что позволит исключить множественность актов законодательства, устранить содержащиеся в них пробелы и противоречия, обеспечить комплексность правового регулирования[266].

В ряде работ Василевич Г.А., Василевич С.Г. рассматривают некоторые аспекты использования информационных технологий для расширения участия граждан в управлении делами государства, исследуют влияние информационных технологий на государственное управление. Внесен ряд предложений, направленных на расширение использования информационных технологий в названной сфере[267]. Авторы обращают внимание на то, что при широком использовании информационных технологий с целью обеспечения права граждан на управление делами государства, должна быть обеспечена защита баз данных, установлена ответственность хранителя за несанкционированное вторжение посторонних лиц к закрытой информации.

Представляют интерес ряд работ Мороз Н.О.[268], в которых дается обзор основных документов, закрепивших право на защиту сведений личного характера в Европейском Союзе, проводится исследование актов институтов Европейского Союза, а также их теоретическое осмысление. Автор приходит к выводу, что правовое закрепление рассматриваемого права и средств его обеспечения в нормативной правовой системе Республики Беларусь позволило бы повысить доверие физических и юридических лиц к информационно-коммуникационным технологиям, что является актуальной проблемой на современном этапе развития. В работе «Договорно-правовая деятельность в борьбе с преступностью в сфере высоких технологий», рассматривая реализацию механизма борьбы с преступностью в сфере высоких технологий, проведен анализ универсальных, региональных и двусторонних соглашений в этой области и сделан вывод, что на современном этапе развития существующий договорно-правовой механизм по борьбе с преступностью в сфере высоких технологий не достаточно эффективен, поскольку требуется заключение универсального международного договора в данной области, который исходил бы из

---

[266] *Абламейко, М.С. Развитие конституционного контроля как важнейшее условие защиты прав граждан / М.С. Абламейко, Г.А. Василевич // Бюллетень нормативно-правовой информации. 2002. № 6. С. 19—28.*

[267] *Василевич, Г.А. Некоторые аспекты использования информационных технологий для расширения участия граждан в управлении делами государства [Электронный ресурс] / Г.А. Василевич // Информационные технологии и право: электронный сборник материалов V Межд. науч.-практ. конф. от 28 мая 2015 г. Режим доступа : http://pravo.by/conf2015/files/proceedings_of_the_conference_2015.pdf. Дата доступа : 24.09.2019.*

[268] *Мороз, Н.О. Оговорки и поправки к международным договорам: на примере международных соглашений по борьбе с киберпреступностью / Н.О. Мороз // Научно-практический журнал «Право.by». 2013. № 1. С. 94—99.*

опыта применения существующих международных соглашений по борьбе с киберпреступностью[269]. Автором обозначена роль ООН в разработке стратегии борьбы с преступностью в сфере высоких технологий. Отмечается и отсутствие комплексных научных работ по теме международно-правового сотрудничества в борьбе с преступностью в сфере высоких технологий[270].

Вопросам защиты тайны частной жизни в Республике Беларусь с учетом ее особенностей в цифровую эпоху уделялось внимание в работах Т.В. Сафоновой, С.С. Лосева, А.А. Бекиш и др. В частности Т.В. Сафонова отмечала, что «имеющиеся нормативные правовые акты, прямо или косвенно регулирующие правовой режим и защиту персональных данных, в полной мере не позволяют гарантировать конституционное право граждан на защиту от незаконного вмешательства в их личную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство»[271]. С этим мнением следует согласиться. Ведь сообщения, передаваемые как электронные данные, имеют много серьезных отличий от обычной телефонной голосовой или телеграфной связи. Эти сообщения содержат несравнимо большее количество персональных данных. При этом абонент является гораздо более уязвимым. В науке до сих пор не найден ответ на вопрос, как защитить тайну сообщений частных лиц, не поступаясь при этом требованиями информационной безопасности в целом.

Одна из наиболее кратких, но в то же время полных публикаций на тему обеспечения тайны сообщений — это статья Н.Н. Федотова[272]. Автор обращает внимание на конфликт интересов информационной безопасности и права человека на тайну связи. Также выделена проблема огромного влияния высокопрофессиональных технических специалистов на общественные отношения нового типа, однако при этом низкой подготовки этих специалистов в области общественных наук, в том числе права. «Высококвалифицированный IT-специалист может напоминать, по мнению Н.Н. Федотова, «варвара среди культурных ценностей». В то же время отмечается «неспособность юристов дать техническим специа-

---

[269] *Мороз, Н.О. Договорно-правовая деятельность в борьбе с преступностью в сфере высоких технологий / Н.О. Мороз // Научно-практический журнал «Право.by». 2010. № 1. С. 41—47.*

[270] *Мороз, Н.О. Роль ООН в координации международного сотрудничества в борьбе с преступностью в сфере высоких технологий / Н.О. Мороз // Научно-практический журнал «Право.by». 2014. № 3. С. 90—95.*

[271] *Сафонова, Т.В. Актуальные проблемы развития института персональных данных в законодательстве Республики Беларусь / Т.В. Сафонова, О.В. Морозова // Наука — образованию, производству, экономике : материалы XVIII (65) Региональной научно-практической конференции преподавателей, научных сотрудников и аспирантов, Витебск : 29—30 марта 2012 г. / Витебский государственный университет им. П.М. Машерова ; редкол.: А.П. Солодков (гл. ред.) [и др.]. Витебск : 2013. С. 352—354.*

[272] *Федотов, Н.Н. Тайна связи против технических средств защиты информации в Интернете [Электронный ресурс] / Н.Н. Федотов // Security Lab by Positive Technologies. Режим доступа : http://www.securitylab.ru/analytics/267646.php. Дата доступа : 05.09.2019.*

листам конкретные рекомендации по вопросам тайны связи». Однако в данной статье практически не упоминается об угрозах тайне сообщений со стороны нарушителей. Не рассматриваются даже явные нарушения со стороны системных администраторов и операторов данных, а лишь пограничные ситуации, в которых не совсем ясно, какое право превалирует: право владельца, собственника информационной системы или сети или право на тайну частной жизни (тайну связи).

Несмотря на предпринятые шаги по совершенствованию законодательства, В.В. Вабищевич отмечает, что в Республике Беларусь недостаточны меры по защите персональных данных. Это проявляется, кроме прочего, в отсутствии уголовной ответственности за разглашение персональных данных и наличии административной ответственности лишь за их умышленное разглашение. Также автор утверждает, что «в правоприменительной практике не устоялись и не сформировались определенные организационные меры по защите персональных данных»[273]. В статье справедливо выделяется проблема того, что «к административной ответственности может быть привлечен правонарушитель только при наличии выраженного в установленном порядке требования потерпевшего или его законного представителя». В.В. Вабищевич обращает внимание на противоречивость регулирования «выражения согласия владельца персональных данных на их разглашение» в белорусском законодательстве.

Некоторые проблемы защиты персональных данных в Республике Беларусь рассматривает Шугай А.А.[274].

В частности, автор указывает на такие проблемы, как отсутствие классификации персональных данных, неурегулированность вопросов ответственности за неправомерное разглашение персональных данных.

На основе анализа положений нормативных правовых актов автор приходит к выводу, что законодательство Республики Беларусь определяет лишь общие вопросы защиты персональных данных (без четкого механизма их реализации), а также точечно регулирует отдельные сферы, в которых используются персональные данные. В другой работе этот автор предпринимает попытку определить место персональных данных в системе объектов гражданских правоотношений. Вопрос отнесения к объектам гражданских правоотношений персональных данных остается дискуссионным.

Следует согласиться с автором, что персональные данные — категория нематериального характера, они неотделимы от личности носителя и подлежат защите в рамках такого объекта гражданских прав, как нематериальные блага. В связи с указанным считаем необходимым внести в п. 1 ст. 151 Гражданского кодекса Республики Беларусь изменения и дополнить перечень нематериальных благ персональными данными.

---

[273] *Вабищевич, В.В. Ответственность за посягательства на персональные данные: новеллы законодательства / В.В. Вабищевич // Юстиция Беларуси. 2018. № 12. С. 70—73.*

[274] *Шугай, А.А. Место персональных данных в системе объектов гражданских правоотношений / А.А. Шугай // Пром.-торг. Право. 2015. №5. С. 40—42.*

Дубко М.А. анализирует вопросы определения размера имущественного вреда, который необходимо признавать существенным при неправомерном завладении компьютерной информацией, предлагая включить соответствующие нормы в примечание к главе 31 УК по аналогии с примечаниями к главе 24 УК, дифференцировав необходимый размер материального вреда (ущерба) в зависимости от того, юридическому или физическому лицу причинен вред. Автором отмечается, что вопрос точного определения наличия существенного вреда при неправомерном завладении компьютерной информацией и установления причинной связи между деянием и последствиями является одним из ключевых и наиболее проблемных в правоприменительной практике[275].

В статье «Уголовно-правовая оценка преступных нарушений авторских прав в сфере программного обеспечения» Марушко Д.А., Абламейко М.С., рассмотрев особенности уголовно-правовой оценки преступных нарушений авторских прав в сфере программного обеспечения, приходят к выводу, что существует значительная потребность в усилении мер предупреждения нарушений законодательства об авторском праве на основе внесения изменений в УК РБ, в котором необходимо сформировать отдельную главу, предусматривающую ответственность за преступления, связанные с интеллектуальной собственностью. А признаки и масштабы ущерба (крупный размер) по ст. 201 УК РБ необходимо определять, ориентируясь на рыночную стоимость лицензионного программного обеспечения с учетом количества проданных копий, а не признавать «размер дохода (ущерба) на сумму, в пятьсот и более раз превышающую размер базовой величины, установленный на день совершения преступления»[276].

Основные дефинитивные проблемы и построение междисциплинарного словаря

Анализ текстов нормативных правовых актов, научной литературы показывает, что долгий период изоляции друг от друга правовых и технических исследований привел к формированию параллельных систем терминологии. Терминология, используемая в технических нормативных правовых актах, не согласуется с терминологией законодательных актов. В итоге термины, используемые IT-специалистами, юристами называются некорректными, а термины, которые применяют юристы, техническим специалистам кажутся слишком абстрактными и не позволяющими идентифицировать субъектов информационных отношений и их объекты.

Поэтому для анализа правового механизма защиты права на тайну сообщений пользователей услуг передачи данных необходимо в первую

---

[275] *Дубко, М.А. Неправомерное завладение компьютерной информацией: существенный вред в составе преступления // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019.*

[276] *Марушко, Д.А. Уголовно-правовая оценка преступных нарушений авторских прав в сфере программного обеспечения / Д.А. Марушко, М.С. Абламейко // Научно-практический журнал «Право.by». 2010. № 4. С. 92—97.*

очередь решить препятствующие этому терминологические проблемы. Наилучшим выходом в такой ситуации было бы построение набора терминов понятных и удобных для специалистов из любой сферы, а также позволяющих исчерпывающе описывать аспекты, входящие в объект и предмет исследования.

Законодательные акты Республики Беларусь не содержат определение понятия «сообщение», несмотря на то, что это понятие многократно используется в нормативных правовых актах. Точное определение мы можем найти только в международном стандарте ISO/IEC 2382:2015, который действует и в Республике Беларусь:

2123141: сообщение (при электронном обмене сообщениями): последовательность битов или символов, которая передается как объект. Примечание — сообщение состоит из двух частей: конверта и содержимого (*en — message*)[277];

2121130: конверт: часть сообщения, которая идентифицирует отправителя сообщения и потенциальных получателей, регистрирует его историю передачи, направляет его последующую передачу системой передачи сообщений и характеризует его содержание (*en — envelope*)[278].

Таким образом, электронное сообщение — это последовательность данных, имеющая определенные характеристики. В белорусском законодательстве содержится как понятие данных, так и понятие передачи данных, которые мы находим в Правилах оказания услуг электросвязи. Из определения сообщения видно, что это объект передаваемый. Поэтому верным будет использовать понятие именно передачи данных.

Передача данных — перенос данных в виде двоичных сигналов средствами электросвязи, как правило, для последующей обработки средствами вычислительной техники[279].

Очевидно, что понятие «передача данных» является более широким и включает в себя и перенос данных как объект, и перенос данных в форме, не имеющей признаков начала и конца. Сообщения могут представлять собой текст, условные знаки, изображения, видеоролики, звукозаписи и другие объекты, имеющие как явный, так и скрытый смысл для отправителя и (или) получателя. Даже пустое сообщение — без какого-либо объекта — должно подлежать праву тайны. Ведь, как известно из указанного выше определения, с точки зрения информатики сообщение не бывает «пустым». Оно содержит в себе, как минимум, конверт.

Следует отметить, что понятие *сообщение* является весьма близким к понятию *корреспонденция*. И лингвистически правильным было бы отождествить понятия сообщение пользователя услуг передачи данных

---

[277] *Информационные технологии. Словарь : ISO/IEC 2382:2015. — ISO/IEC 2382-1:1993 и др. [Электронный ресурс] : введ. РБ 01.05.15. Режим доступа : https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en. Дата доступа : 11.11.2019.*

[278] *Там же.*

[279] *Об утверждении Правил оказания услуг электросвязи [Электронный ресурс] : постановление Совета Министров Респ. Беларусь, 17 авг. 2006 г. № 1055 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019.*

и личная электронная корреспонденция. Однако термин *корреспонденция* традиционно закрепился в сфере деятельности операторов почтовой связи. Для электросвязи аналогичный термин пока не введен. Так, в Законе «О почтовой связи» слово *корреспонденция* употребляется 11 раз. При этом практически во всех случаях уточняется, что речь идет о письменной корреспонденции[280]. В Законе «Об электросвязи» слово *корреспонденция* не употребляется[281].

Также необходимо определить, что следует понимать под тайной. Законодательство Республики Беларусь, несмотря на то, что многократно оперирует понятием тайны, самого этого понятия не определяет. В нормативных правовых актах можно найти лишь определения различных видов тайны (например, коммерческой тайны, тайны почтовой связи), а также близкое понятие «конфиденциальность информации»: *конфиденциальность информации* — требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь[282].

Международный стандарт ISO/IEC 2382:2015 в переводе на русский язык дает два определения конфиденциальности.

4.561 конфиденциальность: защита от вмешательства в частную жизнь или дела отдельной личности в случае неуместного или незаконного сбора и использования данных об этой личности.

4.562 конфиденциальность: свойство, позволяющее не давать права на доступ к информации или не раскрывать ее неуполномоченным лицам, логическим объектам или процессам[283].

Однако здесь же указывается, что определение, данное в пункте 4.561 соответствует английскому слову «*privacy*», а данное в пункте 4.562 — слову «*confidentiality*». Таким образом, защита от вмешательства в частную жизнь или дела отдельной личности в случае неуместного или незаконного сбора и использования данных об этой личности — должна определяться как приватность.

С нашей точки зрения понятие тайны сообщений охватывает обе составляющие — и приватность, и конфиденциальность сообщений. Тайна сообщений ПУПД является разновидностью тайны частной жизни и персональных данных. Частная жизнь и персональные данные — это информация, ограниченная к распространению по своей сути. Для того,

---

[280] *О почтовой связи [Электронный ресурс] : Закон Респ. Беларусь от 15 декабря 2003 г. № 258-З : с изм. доп. от 19 июня 2017 г. № 32-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019.*

[281] *Об электросвязи [Электронный ресурс] : Закон Респ. Беларусь от 19 июля 2005 г. № 45-З : с изм. доп. от 17 июля 2018 г. № 134-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019.*

[282] *Об информации, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь от 10 ноября 2008 г. № 455-З : в ред. от 11 мая 2016 г. № 362-З : с изм. и доп. от 18 мая 2016 г. и 1 июля 2017 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019.*

[283] *Информационные технологии. Словарь : ISO/IEC 2382:2015. — ISO/IEC 2382-1:1993 и др. : введ. РБ 01.05.15. Минск : Белорус. гос. ин-т стандартизации и сертификации, 2015. 201 с.*

чтобы частная жизнь или персональные данные стали тайной, не требуется какого-либо специального юридического акта. Это прямо следует из статьи 28 Конституции Республики Беларусь и других правовых актов. Таким образом, понятие тайны сообщений ПУПД, по нашему мнению, не должно выводиться из понятия коммерческой тайны. Целесообразнее выводить его по аналогии с понятием тайны почтовой связи.

«Тайна почтовой связи — тайна переписки, почтовых отправлений и иных сообщений, входящих в сферу деятельности операторов почтовой связи, не подлежащая разглашению без согласия пользователя услуг почтовой связи, если иное не определено законодательными актами»[284].

При этом следует учитывать, что сообщения ПУПД имеют множество признаков, которые отличают их как от отправлений письменной корреспонденции, так и от телефонных сообщений.

Поэтому **содержание** права на тайну сообщений ПУПД существенно отличается от других похожих прав. В него входят: тайна факта сообщения, тайна его содержания, тайна персональных данных, передаваемых вместе с сообщением. Понятия «сообщение», «тайна сообщений» могут употребляться в законодательстве, регулирующем оказание услуг передачи данных.

Услуга передачи данных (далее УПД) — услуга электросвязи по приему, передаче, обработке и хранению данных[285].

Считаем необходимым отметить, что в данном исследовании велась разработка рекомендаций и предложений по совершенствованию правового механизма защиты права на тайну сообщений, передаваемых в виде двоичных сигналов. Иными словами, рассматриваемые сообщения представляют собой информацию, представленную для обработки средствами вычислительной техники. Данное исследование не охватывало собой тайну телефонных сообщений, тайну телеграмм, телевизионное вещание. В исследовании не рассматривались правовые механизмы защиты тайны сообщений, передаваемых не по сети передачи данных. Сеть передачи данных члены исследовательского коллектива понимают в том смысле, в котором она определена в ст. 1 Закона «Об электросвязи»[286].

Таким образом, хоть право на тайну сообщений ПУПД буквально и не обозначается в законодательстве Республики Беларусь, можно говорить о том, что это право защищается законодательством. Для повышения степени защиты данного права необходимо уточнить терминологию, используемую для характеристики элементов его содержания.

---

[284] *О почтовой связи [Электронный ресурс] : Закон Респ. Беларусь от 15 декабря 2003 г. № 258-З : с изм. доп. от 19 июня 2017 г. № 32-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019.*

[285] *Об утверждении Правил оказания услуг электросвязи [Электронный ресурс] : постановлении Совета Министров Респ. Беларусь, 17 авг. 2006 г. № 1055 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019.*

[286] *Об электросвязи [Электронный ресурс] : Закон Респ. Беларусь от 19 июля 2005 г. № 45-З : с изм. доп. от 17 июля 2018 г. № 134-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019.*

Элементы правового механизма защиты права на тайну сообщений: нормы права, международные, государственные и общественные институты, самозащита прав.

Правовой механизм защиты права на тайну сообщений пользователей услуг передачи данных можно анализировать путем ответов на следующие вопросы:

- Закреплено ли право на тайну сообщений ПУПД подробно и полно в законодательстве Республики Беларусь?
- Существуют ли эффективные способы защиты права на тайну сообщений ПУПД?
- Насколько сложно человеку воспользоваться своим правом на тайну сообщений ПУПД?

Защита прав человека характеризуется рядом признаков: «это определенная деятельность по применению тех или иных способов и средств защиты, совершаемая как государственными органами, так и общественными объединениями либо человеком самостоятельно; направлена на устранение нарушения права, подтверждение либо восстановление оспоренного или нарушенного права; является принудительной по своему характеру, что подразумевает не только само принуждение, но и возможность его применения»[287].

С одной стороны, полнота механизма защиты права строится на трех уровнях. «Первый уровень — это обязательство уважать права человека. Второй уровень — обязательство защищать права человека. Третий уровень — обязательство обеспечивать реализацию конкретных прав»[288].

С другой стороны, в механизме защиты права выделяются различные формы защиты.

6.2. Нормы международного и национального права о тайне сообщений пользователей услуг передачи данных

Нормы международного права

Одним из принципов нормотворческой деятельности в Республике Беларусь является приоритет общепризнанных принципов международного права. Международные договоры являются источником правовой терминологии для проектов нормативных правовых актов Республики Беларусь большей юридической силы. Эти и многие другие причины отводят нормам международного права приоритетную роль в закреплении и защите прав человека.

Традиционно характеристику международных стандартов в сфере прав человека начинают с анализа норм Всеобщей декларации прав человека, а также Международных пактов о правах человека. Статья

---

[287] *Права человека : учеб. пособие / С. А. Балашенко [и др.] ; научн. ред.: С.А. Балашенко, Е.А. Дейкало. Минск : Юнипак, 2015. 200 с.*

[288] *Там же.*

12 Всеобщей Декларации прав человека указывает, что никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции[289]. Примечательный момент в данном положении заключается, на наш взгляд, в указании на недопустимость произвольного вмешательства в сферу личной жизни. По сути, акцентируя внимание на недопустимости произвольного вмешательства, Декларация не исключает того, что такое вмешательство возможно, но на легитимной основе.

Статья 17 Международного пакта о гражданских и политических правах почти дословно воспроизводит данное положение[290]. Принятие этого Пакта и Факультативных протоколов к нему означает не только конкретизацию каталога прав и свобод человека, но и создание контрольных механизмов в названной сфере — Комитета по правам человека, Комитета против пыток и др. В Пакте содержатся положения, регламентирующие границы осуществления прав и свобод человека, указание на необходимость именно законодательного регламентирования ограничений прав, а также цель такого рода отступлений — охрана государственной безопасности, общественного порядка, здоровья или нравственности населения, или прав и свобод других лиц.

Уместно заметить, что вскоре после принятия упомянутых документов международным сообществом были выработаны **Сиракузские принципы** толкования ограничений и отступлений от положений Международного пакта о гражданских и политических правах. Любые ограничения прав, закрепленных в названном Пакте, должны иметь недискриминационный характер, предусматриваться законодательством, преследовать законные цели и быть необходимыми, а также представлять собой наименее ограничительную разумно доступную альтернативу[291].

В числе «факторов, которые сделали в 70—90-е годы XX века проблематику права на неприкосновенность частной жизни актуальной, высту-

---

[289] *Всеобщая декларация прав человека : принята и провозглашена резолюцией 217 А (III) Генеральной Ассамблеи от 10 дек. 1948 г. // Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. — Минск, 2019. Режим доступа : http://etalonline.by/document/?regnum=i04800004&q_id=812781. Дата доступа : 05.07.2019.*

[290] *Международный пакт о гражданских и политических правах : Вступил в силу для Белорусской ССР 23 марта 1976 г. // Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. — Минск, 2019. Режим доступа : http://etalonline.by/document/?regnum=i06600002&q_id=812793. Дата доступа : 29.08.2019.*

[291] *Сиракузские принципы о положениях, касающихся ограничения и умаления прав в Международном пакте о гражданских и политических правах : приняты на сорок первой сессии Комиссии ООН по правам человека 28 сент. 1984 г. // Веб-сайт ООН [Электронный ресурс] / Документы по правам человека. Режим доступа : https://undocs.org/ru/E/CN.4/1985/4. Дата доступа : 29.08.2019.*

пила необходимость защиты персональных данных»[292]. К этому времени стало очевидным, что широкое использование и передача таких данных представляют собой серьезную проблему с точки зрения неприкосновенности частной жизни.

Одним из ранних международных правовых документов, изданных в этой области, является Руководство по защите неприкосновенности частной жизни и трансграничной передаче персональных данных[293]. Оно было принято в 1980 г. и пересмотрено в 2013 г. Организацией по экономическому сотрудничеству и развитию (ОЭСР). Следует отметить, что Республика Беларусь не является членом ОЭСР, однако Совет ОЭСР призывает также страны, не являющиеся членами, реализовывать данные рекомендации. Для Республики Беларусь, по мнению исследовательского коллектива, актуальны такие содержащиеся в Рекомендациях предложения, как «принятие закона, который бы обязывал распорядителей данных сообщать индивидам о взломе их систем», «принятие специального закона о защите неприкосновенности частной жизни», «создание специального органа, ответственного за защиту неприкосновенности частной жизни»[294].

Другим важным международным правовым документом, который направлен на охрану личных данных, выступают Руководящие принципы ООН по регламентации компьютеризированных карточек, содержащих данные личного характера (1990 г.)[295]. В них подчеркивается, что любое лицо, удостоверяющее свою личность, имеет право знать, подвергаются ли касающиеся его данные обработке, получать об этом **сообщения** (ст. 4). Названный документ также содержит положение о том, что в любом законодательстве должен быть указан орган, который гарантирует соблюдение принципов беспристрастности, независимости по отношению к лицам или органам, ответственным за их обработку и применение (ст. 8).

---

[292] *Коннова, Е.В. Право на неприкосновенность частной жизни и осуществление государством негласного сбора персональных данных в сети Интернет // Е.В. Коннова. Е.В. Ходарцевич / Конституционные права и свободы: проблемы интерпретации и реализации в национальных правовых системах. Сборник статей международной научно-практической конференции (Новополоцк, 28—29 октября 2016г.). Новополоцк : ПГУ. Т.1. С. 207—215.*

[293] *Рекомендации Совета ОЭСР, касающиеся Руководства по защите неприкосновенности частной жизни и трансграничной передаче персональных данных 1980 г. (с изм. от 11 июля 2013 года) // Сайт ОЭСР [Электронный ресурс]. Режим доступа : https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf. Дата доступа : 29.08.2019.*

[294] *Рекомендации Совета ОЭСР, касающиеся Руководства по защите неприкосновенности частной жизни и трансграничной передаче персональных данных 1980 г. (с изм. от 11 июля 2013 года) // Сайт ОЭСР [Электронный ресурс]. Режим доступа : https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf. Дата доступа : 29.08.2019.*

[295] *Руководящие принципы, касающиеся компьютеризированных картотек, содержащих данные личного характера : приняты резолюцией 45/95 Генеральной Ассамблеи от 14 дек. 1990 г. // Веб-сайт ООН [Электронный ресурс] / Конвенции. Режим доступа : https://www.un.org/ru/documents/ decl_conv/conventions/computerized_data.shtml. Дата доступа : 05.05.2019.*

Особо следует отметить ряд резолюций Генеральной Ассамблеи ООН, касающихся поощрения, защиты и осуществления прав человека в Интернете, принятые в последние годы. Отдельного рассмотрения заслуживает, например, резолюция, принятая Советом по правам человека 23 марта 2017 года «Право на неприкосновенность частной жизни в цифровой век»[296]. В этом документе отмечается, среди других важных моментов, что развитие информационных и коммуникационных технологий ведет к усилению возможностей правительств, коммерческих предприятий и физических лиц отслеживать, перехватывать и собирать информацию. Резолюция отмечает, что определенные виды метаданных могут раскрывать информацию личного характера, которая может быть не менее конфиденциальной, чем само содержание сообщений, поскольку могут дать представление о поведении, социальных отношениях, индивидуальных предпочтениях и личности человека.

Кроме международных правовых актов в области защиты персональных данных, следует указать на основные документы, изданные в этой области Европейским сообществом. Республика Беларусь не является членом Совета Европы, однако имплементация ряда норм в национальное законодательство повысила бы степень защищенности права на тайну сообщений.

В рамках практики Европейского суда по правам человека право на неприкосновенность личной жизни, закрепленное ст. 8 Европейской конвенции о защите прав человека и основных свобод 1950 г., получило широкое толкование[297]. Именно благодаря такой практике сложилось понимание частной (личной) жизни как емкой категории, которой невозможно дать исчерпывающее определение. Не менее важным необходимо считать следующее обстоятельство: именно Европейский суд указал на то, что государства имеют позитивные обязанности по защите права на неприкосновенность частной жизни в сети Интернет. Государства должны обеспечить разработку и принятие законодательных норм, гарантирующих право на тайну частной жизни[298]. Известно, что в целом ряде правовых отношений один из их участников выступает заведомо слабой стороной. Законодатель не может не учитывать данного обстоятельства и для обеспечения принципа социальной справедливости устанавливает для такой стороны определенные юридические гарантии. На-

---

[296] *Резолюция, принятая Генеральной Ассамблеей 18 дек. 2013 г. Право на неприкосновенность личной жизни в цифровой век // Веб-сайт ООН [Электронный ресурс] / Документы по правам человека. Режим доступа : https://undocs.org/ru/A/RES/68/167. Дата доступа : 05.05.2019.*

[297] *Европейская конвенция по правам человека : принята странами-участниками Совета Европы 4 ноябр. 1950 г. (с учетом протокола №16 от 2 окт. 2013 г. // Сайт Европейского суда по правам человека. Режим доступа : https://www.echr.coe.int/Documents/Convention_RUS.pdf. Дата доступа : 05.05.2019.*

[298] *CASE OF K.U. v. FINLAND [Electronic resource] : The European Court of Human Rights (Fourth Section), 2 December 2008 // European Court of Human Rights. Mode of access : https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-89964 %22]}. Date of access : 20.08.2019.*

пример, при регулировании отношений между производителями работ, товаров и услуг и их потребителями он предоставляет последним ряд материальных и процессуальных льгот и преимуществ. Представляется, что такой же подход должен быть применен и в сфере информационных технологий.

В практике Европейского суда в качестве ответчика по делам упомянутой категории выступают не только государства, но и крупные корпорации. Так, в 2014 году при рассмотрении дела Костеха суд постановил, что поисковые системы типа Google обязаны удалять данные, являющиеся «неточными, неадекватными, неуместными или чрезмерными». Тем самым был установлен стандарт, который потенциально дает возможность применять гораздо более широкие ограничения на публичный доступ к информации, чем это разрешено международными нормами по правам человека или конституционными положениями некоторых стран[299].

Также следует отметить принятую в 1981 году в Страсбурге «Конвенцию о защите физических лиц при автоматизированной обработке персональных данных»[300]. Эта Конвенция открыта и для стран, не являющихся членами Совета Европы, однако по-прежнему не принята Республикой Беларусь. Основной ценностью, которую защищает данная Конвенция, выступает прежде всего право на личное пространство, способом обеспечения которого является неприкосновенность частной информации, принадлежащей лицу, и частных данных, позволяющих достоверно установить лицо и, главное, связаться с ним[301].

В рамках Европейского союза были одобрены сформулированные Европейской комиссией «Основы подхода европейской политики к обеспечению системы информационной безопасности». В этой связи Совет Европейского Союза принял два решения: решение 2002/С 43/02 от 28 января 2002 г. об общем переходе и специальных мерах в сфере сетевой и информационной безопасности[302] и решение 2003/С 48/01 от 18 февраля 2003 г. о европейском подходе в отношении культуры сете-

---

[299] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González [Electronic resource] : Judgment of the Court (Grand Chamber), 13 May 2014 // Court of Justice of the European Union. Mode of access : https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN. Date of access : 20.08.2019.*

[300] *Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера : открыта к подписанию 28 янв. 1981 г. // Интернет-портал Совета Европы. Режим доступа : https://www.coe.int/ru/web/conventions/full-list/-/conventions/rms/0900001680078c46 Дата доступа : 05.06.2019.*

[301] *Дупан, А.С. Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет / А.С. Дупан, А.Б. Жулин. А.К. Жарова и др.; под ред. А.С. Дупан; Нац. исслед. ун-т «Высшая школа экономики». М.: Изд. дом Высшей школы экономики, 2016. 344 с.*

[302] *Council Resolution on a common approach and specific actions in the area of network and information security [Electronic resource] : The Council of the European Union, 28 January 2002 // EUR-lex. Mode of access : https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002G0216(02)&from=EN. Date of access : 20.08.2019.*

вой и информационной безопасности[303]. В них выражалось согласие с предложенными Комиссией мерами в сфере обеспечения информационной безопасности и закреплялись направления их реализации.

Следует отметить, что в праве ЕС имеется целый ряд документов — Директив Европейского Парламента и Совета, регулирующих различные аспекты права на тайну сообщений. Остановимся на некоторых из них. В 1995 году принимается Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных». В данном документе отмечалась его направленность на наполнение содержания и расширение принципов защиты прав и свобод человека, в том числе права на неприкосновенность частной жизни. Спустя короткое время, в начале XXI столетия, в 2002 году Европарламент и Совет Евросоюза принимают Директиву 2002/58/ЕС Об обработке персональных данных и защите конфиденциальности в секторе электронных средств связи. В этом документе одним из примечательных моментов является указание на так называемые шпионские программы, сетевые закладки для сбора и пересылки данных о пользователе компьютера, скрытые идентификаторы и другие подобные устройства, которые могут быть введены в терминал пользователя для доступа к информации или отслеживания деятельности пользователя и тем самым нарушить право на неприкосновенность частной жизни пользователей.

В Директиве 2002/22/ЕС от 7 марта 2002 г. «Об универсальных услугах и правах пользователей в отношении сетей электронных коммуникаций и услуг» нельзя не обратить внимание на положение о том, что нормы национального законодательства, касающегося доступа пользователей к услугам связи или использования их посредством электронных сетей коммуникаций, должны уважать фундаментальные права и свободы граждан, в том числе право на неприкосновенность частной жизни и право на справедливое судебное разбирательство.

В июле 2016 года получила одобрение Директива 2016/1148 ЕС, касающаяся безопасности сети и информационных систем (NIS), целью которой является достижение высокого общего уровня безопасности сетей и информационных систем в рамках ЕС с помощью улучшения возможностей кибербезопасности на национальном уровне, усиления сотрудничества в ЕС, управления рисками и обязательствами по отчетам в случае инцидентов для провайдеров и операторов цифровых услуг. Устанавливалось, что каждое государство-член одобряет национальную стратегию информационной безопасности, определяет компетентные органы по выполнению данной Директивы.

Выработанные в Европейском Союзе подходы к обеспечению информационной безопасности можно рассматривать как европейские рамоч-

---

[303] *Council Resolution on a European approach towards a culture of network and information security [Electronic resource] : The Council of the European Union, 18 February 2003 // EUR-lex. Mode of access : https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32003G0228(01)&from=PL. Date of access : 20.08.2019.*

ные стандарты в данной сфере, которые могут успешно применяться различными странами с учетом их адаптации к особенностям национальных правовых систем.

Показательно, что на эти стандарты ориентируются не только государства в разных частях мира, но и такие международные организации, как Совет Европы. Имеет место и обратное влияние. Так, в 2001 году в Будапеште была подписана Конвенция о преступности в сфере компьютерной информации[304]. В настоящее время этот договор является одним из немногих договоров, в котором участвуют не только страны-члены Совета Европы. Присоединение Республики Беларусь к данной Конвенции позволило бы повысить эффективность сотрудничества стран-участниц Конвенции в борьбе с преступлениями в сфере компьютерной информации. Не следует забывать, что преступления, связанные с нарушением тайны сообщений, во многих случаях являются интернациональными и их раскрытие требует от правоохранительных органов различных государств взаимной правовой помощи.

Особого внимания заслуживает принятый в Европейском союзе в 2016 г. «Общий Регламент по защите персональных данных». Регламент содержит определение персональных данных, субъекта, к которому они относятся, а также устанавливает цели, принципы, общие правила защиты физических лиц в отношении обработки указанных данных и свободного перемещения их в рамках Евросоюза. В Регламенте регулируется статус специальных должностных лиц, таких, как контролер (*controller*) и обработчик (*processor*). В качестве контролера выступает субъект, который самостоятельно или совместно с другими, определяет цели и средства обработки персональных данных. Обработчик (*processor*) обрабатывает персональные данные от имени и по поручению контролера. Контролеры и обработчики в рамках своих программ отчетности обязаны назначить инспектора по защите данных (Data Protection Officer)[305]. Такое назначение осуществляется в случаях, если соответствующая обработка проводится государственным органом либо основная деятельность контролера или обработчика связана с такой обработкой, которая по своему охвату, целям и сути, требует крупномасштабного, регулярного и систематического мониторинга субъектов данных, а также при обработке специальной категории данных.

Возможность применения норм Регламента к гражданам третьих стран, не входящих в Европейский Союз, обуславливает чрезвычайную важность данного международного правового документа для белорус-

---

[304] *Конвенция о компьютерных преступлениях : открыта к подписанию 23 ноября 2001 г. // Интернет-портал Совета Европы. Режим доступа : https://www.coe.int/ru/web/conventions/full-list/-/conventions/rms/0900001680081580. Дата доступа : 05.06.2019.*

[305] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Electronic resource] : the European Parliament and of the Council of the European Union // EUR-lex. Mode of access : https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&qid=1571013428568&from=EN. Date of access : 20.08.2019.*

ского законодателя. Нет сомнения, что европейский опыт требует внимательного изучения, имея в виду то обстоятельство, что рано или поздно соответствующий механизм защиты персональных данных придется вводить и в отечественной правовой системе.

Проблематика нормативной регламентации защиты персональных данных, безусловно, требует специального изучения, которое, кстати говоря, ведется современной юриспруденцией весьма интенсивно. В этой связи следует заметить, что для понимания специфики реализации права на тайну сообщений в сети Интернет уместно обращение не только к международным правовым документам, но и к позициям, которые отражают мнение экспертов в области прав человека, исследованиям ученых в данной сфере. С этой точки зрения заслуживает внимания Доклад Франка Ля Рю — Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение на Семнадцатой сессии Совета по правам человека Генеральной Ассамблеи ООН[306]. В частности, Франк Ля Рю характеризует проблему кибератак и отсутствие надлежащей защиты права на неприкосновенность частной жизни и защиту данных.

Как показывает опыт, посягательства на неприкосновенность частной жизни имеют место со стороны как органов публичной власти, так и крупных корпораций, а также частных лиц. Например, государства использовали такие популярные социальные сети, как Facebook для выявления и отслеживания деятельности правозащитников и членов оппозиции и в некоторых случаях узнавали имена пользователей и пароли для получения доступа к частной переписке пользователей[307].

Вопрос о правовом регулировании тайны сообщений и защиты персональных данных актуален не только на глобальном, но и на региональном уровне. В Содружестве независимых государств развитие сферы коммуникаций имеет давнюю историю. Современный этап данного развития определяется положениями Стратегии сотрудничества государств-участников СНГ в построении и развитии информационного общества на период до 2025 года, утвержденной Решением Совета глав правительств СНГ от 28.10.2016 года[308].

---

[306] *Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Франка Ла Рю : представлен на семнадцатой сессии Совета по правам человека // Веб-сайт ООН [Электронный ресурс] / Документы по правам человека. Режим доступа : https://undocs.org/pdf?symbol=ru/A/HRC/17/27 Дата доступа : 02.04.2019.*

[307] *Филимонова, Д. Защита персональных данных: обуза для бизнеса и тех, кому «нечего скрывать»? [Электронный ресурс] / Д. Филимонова // Сайт Федерации профсоюзов Беларуси. Режим доступа : https://1prof.by/news/economy/zashchita_personalnykh_dannykh_obuza_dlya_biznesa_i_tekh_komu_nechego_skryvat.html Дата доступа : 07.05.2019.*

[308] *Стратегия сотрудничества государств-участников СНГ в построении и развитии информационного общества на период до 2025 года [Электронный ресурс] : [утверждена в г. Минске 28.06.2016 г.] // Сайт Регионального содружества в области связи. Режим доступа : http://www.rcc.org.ru/uploads/20180628/strategiya_sng-infobshestvo-2025.pdf Дата доступа : 14.09.2019.*

Особое место здесь, безусловно, занимают правовые регуляторы, направленные на оптимизацию функционирования сегмента информационной безопасности в СНГ в условиях современных вызовов. Так, в 2001 г. на уровне СНГ было заключено Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в информационной сфере. В этой связи стоит отметить также подписанное главами правительств СНГ в 2013 году Соглашение о сотрудничестве государств-участников СНГ в области обеспечения информационной безопасности[309]. Соглашение предусматривает проведение совместных скоординированных мероприятий, направленных на обеспечение информационной безопасности в государствах-участниках СНГ посредством организации взаимодействия и сотрудничества его участников.

В рамках ОДКБ имеется один договор — Протокол о взаимодействии государств-членов ОДКБ по противодействию преступной деятельности в информационной сфере от 23 декабря 2014 г.

В ноябре 2018 г. Комитет по правам человека в Заключительных замечаниях по пятому периодическому докладу Беларуси отметил, что «государству следует обеспечить, чтобы во всех решениях, ограничивающих право на свободу и личную неприкосновенность, неукоснительно соблюдались принципы законности и соразмерности, а также гарантировать полное соблюдение процессуальных прав»[310]. Мы согласны с такой точкой зрения и считаем, что если бы правовой механизм защиты тайны сообщений ПУПД совершенствовался с учетом положений ключевых международных актов в данной сфере, показатели доверия к правоохранительным органам, показатели чувства безопасности среди белорусских пользователей программ для передачи сообщений существенно бы улучшились.

Анализ норм международного права помогает в данном исследовании выявить причины несовершенства национального правового механизма защиты прав, выявить причины низкого доверия к национальным правовым гарантиям права на тайну сообщений ПУПД. Следует обратить внимание на тот факт, что Республика Беларусь не является участницей ряда ключевых международных договоров, направленных на защиту прав пользователей компьютерных систем, сетей и ресурсов. Включение норм данных актов в национальное законодательство позволило бы существенно повысить степень защищенности права на тайну сообщений ПУПД.

---

[309] *Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности [Электронный ресурс] : [заключено в г. Санкт-Петербурге 20.11.2013 г.] / Нац. центр правовой информ. Респ. Беларусь. Минск, : 2019. Режим доступа : http://etalonline.by/document/?regnum=i04800004e&q_id=812781 Дата доступа : 05.07.2019.*

[310] *Заключительные замечания по пятому периодическому докладу Беларуси [Электронный ресурс] : Комитет по правам человека, 22 ноября 2018 г. // Веб-сайт ООН [Электронный ресурс] / Международные договоры по правам человека. Режим доступа : http://docstore.ohchr.org/ . Дата доступа : 05.07.2019.*

Нормы национального права

Наше государство только приступает к разработке и внедрению в законодательной и исполнительной областях комплексного подхода к обеспечению защиты права на тайну сообщений ПУПД. Поэтому весьма важно сосредоточить внимание как на тех нормах, которые позволяют говорить о полном и подробном закреплении права на тайну сообщений ПУПД в законодательстве, так и на тех пробелах и недостатках законодательства, которые еще предстоит восполнить.

Право на тайну сообщений ПУПД следует из формулировки ст. 28 Конституции Республики Беларусь[311]. Конституция защищает тайну абсолютно любых сообщений, независимо от средств, технологии их создания и передачи. Очевидно, что сообщения ПУПД попадают в категорию «иных сообщений». При этом тайна сообщений рассматривается как часть права на личную жизнь.

Более подробно раскрывает понятия частной жизни и сообщений ст. 18 ***Закона «Об информации, информатизации и защите информации»*** — информация о частной жизни физического лица и персональные данные. Согласно этой статье, в состав информации о частной жизни включаются, кроме прочего, сведения, составляющие личную и семейную тайну, тайну телефонных переговоров, почтовых и иных сообщений, сведения, касающиеся состояния здоровья. Согласно абзацу второму этой же статьи «*сбор, обработка, хранение информации о частной жизни физического лица и персональных данных, а также пользование ими осуществляются с письменного согласия данного физического лица, если иное не установлено законодательными актами Республики Беларусь*»[312]. Таким образом, поскольку тайна сообщений ПУПД является составной частью информации о частной жизни, то сбор, обработка, хранение информации, содержащейся в сообщениях ПУПД, может осуществляться только с письменного согласия физического лица, если иное не установлено законодательными актами Республики Беларусь. Также в этой статье детализируется понятие, употребляемое в ст. 28. Конституции «незаконное вмешательство в личную жизнь» — это сбор, обработка, хранение информации о частной жизни физического лица без его письменного согласия или без установления законодательного акта, а также в нарушение порядка обработки такой информации, установленного законодательными актами.

Как отмечалось выше, сообщение, передаваемое как электронные данные, — это не только видимая его часть, но также и конверт, который содержит, кроме прочего, персональные данные отправителя, а иногда и

---

[311] *Конституция Республики Беларусь : с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г. и 17 окт. 2004 г. Минск : Нац. центр правовой информ. Респ. Беларусь, 2016. 62 с.*

[312] *Об информации, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь от 10 ноября 2008 г. № 455-З : в ред. от 11 мая 2016 г. № 362-З : с изм. и доп. от 18 мая 2016 г. и 1 июля 2017 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019.*

получателя сообщения. Поэтому вопрос тайны сообщений как разновидности тайны частной жизни нельзя рассматривать в отдельности от тайны персональных данных. Виды информации, относящиеся к категории персональных данных, перечислены в ст.ст. 8—10 Закона «О регистре населения»[313]. Общие начала защиты персональных данных содержит ст. 32 Закона «Об информации, информатизации и защите информации». Исходя из ее содержания применительно к сообщениям ПУПД, часть персональных данных пользователя должна защищаться с момента их предоставления поставщику услуг либо с начала оказания услуг передачи данных (в зависимости от того, что наступит ранее) и вплоть до удаления персональных данных с устройств хранения данных поставщика услуг передачи данных либо до прекращения оказания услуг (в зависимости от того, что наступит ранее). Другая часть персональных данных должна быть защищена с момента создания сообщения пользователем и вплоть до уничтожения информации, составляющей данное сообщение. Статья 32 Закона запрещает не только разглашение, но и использование персональных данных, полученных в нарушение законодательных актов Республики Беларусь.

Многие положения, относящиеся к тайне сообщений, закрепляет Закон «Об электросвязи»[314]. Статья 4 данного Закона провозглашает тайну телефонных и иных сообщений в качестве одного из принципов деятельности в области электросвязи. Соблюдение тайны телефонных и иных сообщений является обязанностью оператора согласно ст. 42 указанного закона. Обязанность оператора электросвязи корреспондирует право пользователя на тайну телефонных и иных сообщений. Данное право гарантируется ст. 54 Закона. Пользователь может защищать свое право на тайну сообщений в суде. При этом пользователь может требовать возмещения ущерба и морального вреда, нанесенных нарушением права на тайну сообщений. Эти права пользователя услуг электросвязи закрепляет ст. 46 Закона.

К правилам, обеспечивающим защиту права на тайну сообщений ПУПД, следует также отнести нормы, обязывающие собственников (владельцев) информационных систем применять средства технической и криптографической защиты информации[315].

---

[313] *О регистре населения [Электронный ресурс] : Закон Респ. Беларусь от 21 июля 2008 г. № 418-З : в ред. от 9 янв. 2019 г. № 170-З : с изм. и доп. от 18 апр. 2019 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019.*

[314] *Об электросвязи [Электронный ресурс] : Закон Респ. Беларусь от 19 июля 2005 г. № 45-З : с изм. доп. от 17 июля 2018 г. № 134-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019.*

[315] *О некоторых мерах по совершенствованию защиты информации : Указ Президента Респ. Беларусь, 16 апр. 2013 г. № 196 : с изм. доп. от 1 июня 2018 г. № 239 // Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019. Режим доступа : http://etalonline.by/document/?regnum=p31300196&q_id=812717. Дата доступа : 05.09.2019.*

Таким образом, несмотря на отсутствие действующего законодательного акта о защите персональных данных, можно сделать вывод, что законодатель уделяет значительное внимание праву человека на тайну электронных сообщений. Однако в борьбе с киберправонарушениями значительная роль должна отводиться ответственности за нарушенное право. Именно ответственность выполняет воспитательную функцию и тем самым свидетельствует о наиболее полной защите права.

Право на неприкосновенность частной жизни защищено ст. 179 УК Республики Беларусь.

Специальной нормой, устанавливающей уголовную ответственность за нарушения права человека, закрепленного в ст. 28 Конституции, является ст. 203 УК Республики Беларусь[316]. Статья 203 защищает право на тайну сообщений ПУПД от посягательств со стороны лиц, которые могут незаконно ознакомиться с ним, которым тайна сообщений стала известна в связи с их служебным или должностным положением (сотрудники организаций-поставщиков интернет-услуг, операторов электросвязи, сотрудники правоохранительных органов) и которые могут разгласить эту тайну иным лицам.

Если ознакомление с содержанием сообщения ПУПД произошло в результате преодоления системы защиты компьютерной информации, то в действие вступает ст. 349 УК Республики Беларусь. При этом нарушение конституционного права на тайну личной (частной) жизни, права на тайну сообщений ПУПД является существенным вредом.

Если тайна сообщения была нарушена таким образом, что не просто произошло ознакомление с его содержанием, а была создана копия сообщения без согласия отправителя/получателя, либо злоумышленник замаскировался под получателя и получил сообщение вместо него, либо сообщение было перехвачено в ходе его передачи по каналам электросвязи, то в этом случае право на тайну сообщений защищается ст. 352 Уголовного кодекса.

Таким образом, на первый взгляд, любые действия, направленные на нарушение тайны сообщений ПУПД, запрещены Уголовным кодексом Республики Беларусь. Однако остается открытым вопрос, ***чувствует ли человек себя защищенным в результате действия вышеуказанных статей***.

Законодательство Республики Беларусь защищает тайну сообщений ПУПД не только от преступных посягательств. Если размер причиненного вреда, степень общественной опасности даже не превышают тех порогов, которые устанавливаются Уголовным кодексом, может наступать административная ответственность за нарушение тайны сообщений, в том числе за разглашение персональных данных. Это предусматривают ряд

---

[316] *Уголовный кодекс Республики Беларусь : принят Палатой представителей 2 июня 1999 г.: одобрен Советом Республики 24 июня 1999 г.: с изм. и доп.: текст по состоянию на 18 янв. 2019 г. // Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. — Минск, 2019. Режим доступа : http://etalonline.by/document/?regnum=hk9900275&q_id=812636. Дата доступа : 05.09.2019.*

статей КоАП Республики Беларусь, которые весьма схожи по содержанию с соответствующими статьями Уголовного кодекса. Среди них следует выделить: ст. 22.6. Несанкционированный доступ к компьютерной информации; ст. 22.13. Разглашение коммерческой или иной охраняемой законом тайны либо персональных данных[317].

Вышеизложенная характеристика комплекса правовых норм Республики Беларусь, защищающих тайну сообщений ПУПД, показывает, что у пользователя есть определенная нормативная база для защиты тайны своих сообщений от посягательств.

Остается вопрос, насколько пользователь может защитить свое право на тайну, используя эти нормы права. Не случится ли так, что шпион, кибersталкер, преследователь, хакер, мошенник не будут привлечены к ответственности; а даже если они и будут привлечены к ответственности, то возместят ли ущерб, нанесенный их противоправными действиями пользователю? Не случится ли так, что оператор / поставщик услуг передачи данных сможет использовать сведения, содержащиеся в сообщениях пользователей, по своему усмотрению; что количество субъектов, которым оператор уполномочен разглашать информацию, таково, что фактически отменяет обязанность соблюдать тайну сообщений? В последнее десятилетие также остро стоит вопрос о том, не находится ли пользователь информационного ресурса, информационной системы в изначально слабой, вынужденной позиции и не способен защитить свои права на тайну, которые нарушает собственник (владелец) такого ресурса или системы.

Не менее важным является вопрос, насколько эффективны нормы по защите права на тайну сообщений, может ли гражданин быть относительно уверен в неотвратимости ответственности виновных в нарушении его права. Социологические опросы, проводившиеся в Республике Беларусь, показывают, что доверие к указанным правовым нормам не самое высокое.

В январе—феврале 2019 г. белорусская правозащитная организация Human Constanta и некоммерческая общественная организация Baltik Internet Policy Iniciative провели два опроса белорусских интернет-пользователей «Онлайновый активизм» и «Цифровые права и свободы»[318]. Около 1000 человек (всего было опрошено 910 человек, из них 47 % мужчин и 51 % женщин) выразили свое отношение к правам человека в цифровой среде. Согласно данным опросам, для 52 % пользователей он-

---

[317] *Кодекс Республики Беларусь об административных правонарушениях : принят Палатой представителей 17 декабря 2002 г.: одобрен Советом Республики 2 апреля 2003 г.: с изм. и доп.: текст по состоянию на 3 авг. 2019 г. // Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019. Режим доступа : http://etalonline.by/document/?regnum=hk0300194&q_id=812649. Дата доступа : 05.10.2019.*

[318] *Онлайновый активизм и цифровые свободы: Беларусь 2019 [Электронный ресурс] : Исследование: онлайновый активизм и цифровые права // Human Constanta. Режим доступа : https://humanconstanta.by/wp-content/uploads/2019/04/HumanConstanta_Presentation_29.03.19.pdf. Дата доступа : 05.09.2019.*

лайновые ресурсы и сервисы помогают поддерживать социальные связи; 92 % пользователей Интернета считают, что осведомлены в вопросах защиты персональных данных; 49 % опрошенных считают, что наиболее востребованными цифровыми навыками в Беларуси являются умение обеспечивать безопасность и защиту персональных данных.

Более 70 % ответивших могут предпринять основные шаги для защиты устройств с помощью антивирусов и паролей и знают, как реагировать, если компьютер заражен вирусом. Однако далеко не все часто проверяют конфигурацию систем безопасности устройств (54 %), могут настроить или изменить параметры безопасности цифровых устройств (54 %), используют разные пароли доступа (64 %).

В то же время 81 % респондентов считают неприкосновенность частной жизни важным цифровым правом человека.

Только 23 % опрошенных на вопрос «Если Вы столкнетесь с проблемой нарушения безопасности Вашего устройства или утечкой информации, к кому Вы обратитесь?» ответили, что «обратятся в специальные подразделения МВД. Только 14 % обратились бы в такой ситуации в правозащитные органы. Абсолютное же большинство ответивших обратились бы к знакомым специалистам, компьютерным сервисам или друзьям»[319]. ***С нашей точки зрения это очень важный показатель, демонстрирующий неготовность пользователей услуг передачи данных пользоваться правовыми мерами по защите тайны сообщений***.

Положительно оценивают законодательный запрет на публичное раскрытие информации о частной жизни конкретных людей 48 % респондентов. В то же время 26 % считают, что такой запрет относителен. Однако интересно, что целых 12 % считают, что такой запрет недопустим[320].

Из этих данных становится ясно, что пользователи услуг передачи данных испытывают надобность в совершенствовании механизма защиты тайны их сообщений. При этом пользователи не отдают предпочтение институциональным правовым мерам защиты их права. Соответственно, в данном исследовании мы постарались уделить большое внимание правовым неинституциональным мерам защиты.

6.3. Правовые и криптографические меры защиты тайны сообщений ПУПД: нерешенные противоречия

Пользователь, передающий данные, составляющие его сообщение, заинтересован, чтобы с содержанием сообщения мог ознакомиться только тот получатель, которому оно адресовалось, т. е. интересом и правом пользователя является тайна сообщения. Компьютерные технологии передачи сообщений дали человеку множество невероятных возможностей: доставка сообщений мгновенно, возможность реагировать на сообщения мгновенно, возможность восстанавливать даже утрачен-

---

[319] *Там же.*

[320] *Там же.*

ные сообщения и т.п. Эти возможности оказались сопряженными с неизвестными ранее рисками и угрозами для тайны сообщений. Большая их часть связана с тем, что пользователю не хватает знаний, чтобы понять всю технологию создания и передачи сообщения и, тем более, не хватает знаний, чтобы предвидеть все возможные способы нарушения тайны сообщений.

Риски нарушения тайны сообщений присутствуют на всех этапах создания, передачи и хранения сообщения. Отследить этот путь сложно еще и потому, что при передаче сообщений пользователи вступают, как минимум, в две группы правоотношений. Это, во-первых, правоотношения с собственником (владельцем) компьютерной программы, предназначенной для передачи сообщений, а во-вторых, с оператором услуг передачи данных. Можно обозначить основные точки, с которых может произойти разглашение тайны сообщений. Это, во-первых, компьютерная программа отправителя, компьютерная программа получателя, базы данных на сервере и иная инфраструктура собственника (владельца) компьютерной программы, предназначенной для передачи сообщений; во-вторых, это базы данных на сервере и иная инфраструктура оператора услуг передачи данных.

Реализовать угрозы тайне сообщений могут несколько категорий субъектов. Их можно назвать общим термином — киберправонарушители. Их действия могут составлять преступление или административное правонарушение.

Лица, преодолевающие системы защиты компьютерной информации. В литературе, а также технических нормативных правовых актах, их часто называют хакерами, или взломщиками[321]. Причины, по которым киберпреступники могут пытаться получить доступ к информации о частной жизни и персональным данным могут быть самые различные. Ксинган Ли выделяет целых 29 мотивов, которые могут двигать хакерами. Это и различного рода корыстные мотивы, психологические проблемы, подготовка к совершению других преступлений[322]. Независимо от мотива, по которому злоумышленник нарушил тайну сообщений правомерного пользователя, важно чтобы данный пользователь имел все возможности восстановить свои права.

Теоретически подробное установление правовых запретов на общественно опасные, вредные действия должно создавать такие возможности. И белорусское законодательство содержит такие запреты.

Для того, чтобы право на тайну сообщений могло считаться защищенным от посягательств киберпреступников, пользователи должны иметь возможность без затруднений воспользоваться инструментами, которые им предоставляет законодательство. По данным Управления

---

[321] *Информационные технологии. Словарь : ISO/IEC 2382:2015. — ISO/IEC 2382-1:1993 и др. [Электронный ресурс] : введ. РБ 01.05.15. Режим доступа : https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en. Дата доступа : 11.11.2019.*

[322] *Xingan Li. A Review of Motivations of Illegal Cyber Activities / Li Xingan // Criminology & Social Integration Journal. 2017. Vol. 25, No 1. P. 110—126.*

по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь, количество преступлений в сфере высоких технологий выросло за 2018 год на 53 %. При этом наиболее существенный рост отмечался в категории преступлений — несанкционированный доступ к компьютерной информации (+97 %)[323]. Из этого видно, что угроза тайне сообщений ПУПД со стороны преступников существенно растет. Однако речь идет только о выявленных преступлениях. О реальном количестве преступлений, связанных с посягательством на тайну сообщений, в силу высокой латентности можно только догадываться. Устные беседы с пользователями, обнаружившими взлом своих учетных записей, с помощью которых они осуществляли общение в Интернете, показывают, что очень немногие из них обращаются за помощью в правоохранительные органы.

Помимо возможности обращения в правоохранительные органы, пользователь сети передачи данных может также осуществлять защиту своих прав в судебном порядке. Даже если лицо, ответственное за нарушение, не привлечено к уголовной или административной ответственности, это не лишает пользователя права добиваться возмещения нанесенного ему нарушением тайны сообщений вреда в гражданско-правовом порядке.

Недобросовестные собственники, владельцы компьютерных программ и оборудования, предназначенных для обмена электронными сообщениями. Практика показывает, что наиболее частыми целями нарушения тайны сообщений ПУПД со стороны обработчиков больших данных (*big data*)[324] являются последующая продажа полученной информации, глубинный анализ данных (*data mining*) и коммерческое использование его результатов (прежде всего таргетированная реклама), предсказание социальных процессов, в том числе предсказание поведения человека. Обработка больших данных — это вид деятельности, который пока недостаточно описан в литературе в силу своей новизны и покрытости завесой коммерческой тайны биг-дэйта компаний. Это обстоятельство неоднократно замечается пользователями интернет-ресурсов, однако оно очень трудно доказуемо. Пользователь замечает, что он не обращался к интернет-ресурсам, содержащим информацию о тех или иных товарах и услугах, а лишь упоминал о желании приобрести товар или получить услугу в личных сообщениях при беседах с другими пользователями посредством встроенных в информационные ресурсы программ передачи сообщений, а затем неожиданно получал рекламу

---

[323] *Статистика Управления по раскрытию преступлений в сфере высоких технологий [Электронный ресурс] // Министерство внутренних дел Республики Беларусь. Режим доступа : https://www.mvd.gov.by/ru/page/upravlenie-po-raskrytiyu-prestuplenij-v-sfere-vysokih-tehnologij-upravlenie-k/stastistika-urpsvt. Дата доступа : 29.06.2019.*

[324] *Manyika, J. Big data: The next frontier for innovation, competition, and productivity [Electronic resource] / J. Manyika and others // McKinsey Global Institute. Mode of access : https://www.mckinsey.com/~/media/McKinsey/BusinessFunctions/McKinsey Digital/Our Insights/BigdataThenext frontierforinnovation/MGI_big_data_full_report.ashx. Date of access : 20.04.2019.*

товара или услуги, о которой шла речь. Логично пользователь приходил к выводу, что собственник (владелец) информационного ресурса ознакомился с содержанием переданного сообщения, а соответственно, нарушил тайну сообщений. В большинстве случаев субъекту, анализирующему большие данные, даже нет необходимости прочитывать содержание сообщений, а достаточно ознакомиться с содержанием конверта: кому человек отправлял сообщения, от кого их получал, с какой частотой, в связи с какими датами, с помощью каких устройств и т.п. Например, если, получив сообщение на стационарное устройство от начальника, человек перешел на общение с помощью мобильного устройства и его местоположение меняется, можно прийти к выводу, что человек уехал на работу и его определенное время не будет дома. Если человек получает сообщения от друга-врача, а после этого пишет сообщения нелегальным распространителям лекарственных средств, можно прийти к выводу, что человек скрывает какую-то болезнь. Можно только догадываться, насколько полную и подробную информацию может дать о человеке анализ большого количества данных о его сообщениях.

Большинство операторов отрицает факт прочтения сообщений и утверждает касательно таргетированной рекламы, что она была лишь случайным совпадением. В таких ситуациях пользователю очень трудно доказать факт нарушения своего права на тайну. Другие компании признают факты ознакомления с содержанием сообщений пользователей, всячески оправдывая свои действия. Обычно приводятся оправдания следующего характера: забота о нуждах пользователя, профилактика правонарушений, стремление повысить качество услуг и др. В настоящее время формируются две основные концепции разрешения данной проблемы. Согласно первой, собственники информационных ресурсов имеют право использовать данные пользователей этих ресурсов в качестве платы за бесплатное пользование информационным ресурсом. К тому же пользователь сам соглашается с обработкой своих данных, проставляя соответствующие символы в соответствующих разделах пользовательского соглашения. Согласно второй концепции, персональные данные в силу своей природы являются принадлежащими человеку, и их защита подразумевает полный контроль человека над своими персональными данными. Персональные данные не могут быть переданы «в любое использование», а человек имеет право знать о любой операции со своими персональными данными. Аргумент о том, что предоставление своих персональных данных является платой за пользование информационным ресурсом, также парируется тем, что персональные данные имеют такую природу, которая не позволяет оценить их стоимость и никоим образом нельзя их предоставление считать равнозначной платой за пользование ресурсом. Человек имеет право на часть дохода от обработки своих персональных данных.

На эту проблему обращает внимание и специальный докладчик по вопросу о праве на неприкосновенность частной жизни. В пункте 60 своего доклада Специальный докладчик призывает правительства объе-

диняться вокруг позиции законодательного запрещения таких несоразмерных, неоправданных мер вторжения в сферу частной жизни, как сбор больших объемов данных, масштабное проникновение в компьютерные сети и несанкционированное прослушивание[325].

Отдельного рассмотрения заслуживает, например резолюция, принятая Советом по правам человека 23 марта 2017 г.[326] В этом документе отмечается, что развитие информационных и коммуникационных технологий ведет к усилению возможностей правительств, коммерческих предприятий и физических лиц отслеживать, перехватывать и собирать информацию.

Законодательство Республики Беларусь также пока не решает вышеописанную проблему. Нормы Уголовного кодекса и Кодекса об административных правонарушениях формально такими действиями не нарушаются. Ведь, как правило, соблюдается формальность дачи письменного согласия на обработку персональных данных. И оператор данных может утверждать, что соблюдает требования закона. Возможно, в большей степени защитит права пользователя на тайну сообщений ***будущий Закон Республики Беларусь «О защите персональных данных»***[327]. Анализ статьи 5 проекта данного закона показывает, что согласие субъекта персональных данных должно будет содержать также цель или цели сбора, обработки, распространения, предоставления персональных данных. Это существенный шаг по предупреждению нарушений со стороны оператора данных. По нашему мнению, очень важно обязать подробно раскрывать цели обработки персональных данных, чтобы согласие субъекта не сводилось к простой формальности подписания дополнительного бессмысленного документа, который не дает никаких больших гарантий защиты прав пользователя, а лишь дополнительное алиби оператору. Также важно учитывать, что современные технологии глубинного анализа данных позволяют идентифицировать физическое лицо даже после обезличивания данных. Поэтому правовая защита тайны сообщений и прежде всего их конвертов должна действовать и после обезличивания данных.

Субъекты, получающие несанкционированный доступ к базам данных операторов, поставщиков услуг электросвязи. Выше уже говорилось о том, что взломщики (хакеры) могут получить доступ к сообщениям

---

[325] *Доклад Специального докладчика по вопросу о праве на неприкосновенность частной жизни Джозефа Каннатаки : представлен на тридцать первой сессии Совета по правам человека // Веб-сайт ООН [Электронный ресурс] / Документы по правам человека. Режим доступа : https://undocs.org/ru/A/HRC/31/64. Дата доступа : 31.04.2019.*

[326] *Резолюция, принятая Советом по правам человека 23 марта 2017 года № 34/7 Право на неприкосновенность частной жизни в цифровой век // Веб-сайт ООН [Электронный ресурс] / Документы по правам человека. Режим доступа : https://undocs.org/pdf?symbol=ru/A/HRC/RES/34/1. Дата доступа : 29.06.2019.*

[327] *Проект Закона Республики Беларусь «О персональных данных» // Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019. Режим доступа : http://forumpravo.by/files/proekt_zakona_o_personalnih_dannih.pdf. Дата доступа : 09.10.2019.*

путем не только преодоления системы защиты компьютеров пользователей, но и инфраструктуры операторов связи. Однако особо следует обратить внимание на киберправонарушителей, организованно устанавливающих постоянную возможность доступа к сетям передачи данных и находящихся в них базам данных операторов. Речь идет о зарегистрированных зарубежными правоохранительными органами случаях недобросовестности поставщиков оборудования для операторов связи. Некоторые поставщики оборудования даже после установки и использования данного оборудования в сетях связи заказчика оставляют за собой техническую возможность доступа к информации, передаваемой по данным сетям. В связи с этим в некоторых зарубежных странах, в частности США, Австралии, Новой Зеландии было дополнено законодательство о закупках оборудования для сетей связи[328]. В Республике Беларусь заказчиком строительства волоконно-оптических линий связи, строительства сетей стационарного широкополосного доступа, строительства сетей передачи данных (точек доступа) по технологии Wi-Fi, проектирования, строительства и эксплуатации единой сети сотовой подвижной электросвязи по технологии LTE (4G) — является Министерство связи и информатизации и подчиненные ему организации. Осуществление полномочий по закупке оборудования для указанных мероприятий осуществляется этими субъектами согласно Указу Президента Республики Беларусь от 22 декабря 2014 г. № 612[329].

Предполагается, что для большей защищенности прав и интересов граждан Республики Беларусь, в том числе для большей защиты их права на тайну сообщений, необходимо дополнить данный Указ следующим: *пункт 1.6 Указа* дополнить абзацем «требования к уровню защиты информации, уровню защиты коммерческой и иной охраняемой законом тайны, уровню защиты интеллектуальной собственности, уровню защиты частной жизни и персональных данных»;

пункт 1.12 Указа «критериями оценки и сравнения предложений участников в целях проведения процедур государственных закупок помимо критериев, определенных иными актами законодательства, регулирующими отношения в области государственных закупок, являются: ...» дополнить абзацем «отсутствие правонарушений, связанных с нарушением коммерческой и иной охраняемой законом тайны, с нарушени-

---

[328] *Securing the Information and Communications Technology and Services Supply Chain : Executive Order of the President of the USA Nr. 13873 of May 15, 2019 [Electronic resource] : official portal of the White House. Mode of access : https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/. Date of access : 10.10.2019.*

[329] *Об осуществлении государственных закупок в сферах информатизации, информационно-коммуникационных технологий и телекоммуникаций : Указ Президента Респ. Беларусь, 22 дек. 2014 г. № 612 : с изм. доп. от 23 марта 2016 г. № 106 // Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. Минск, 2019. Режим доступа : http://pravo.by/document/?guid=3871&p0=P31400612. Дата доступа : 01.10.2019.*

ем прав интеллектуальной собственности, с нарушением тайны частной жизни и персональных данных»;

пункт 1.15 Указа «существенными условиями договоров, заключаемых для реализации мероприятий программ информатизации, помимо иных условий, установленных в соответствии с законодательством, являются: ...» дополнить абзацем «гарантии соблюдения коммерческой и иной охраняемой законом тайны, прав интеллектуальной собственности, тайны частной жизни и персональных данных».

В соответствии с дополнениями Указа включить в типовую форму технического задания по мероприятию государственной программы информатизации и ее подпрограмм соответствующие положения.

Проблема разграничения ответственности пользователя компьютерной программы и разработчика компьютерной программы. Если тайна сообщения ПУПД все же была нарушена, возникает спор, по чьей вине это произошло. Если пользователь сообщил каким-либо способом кому-либо данные, необходимые для входа в аккаунт для передачи сообщений, то он, безусловно, не может предъявлять претензии к собственнику (владельцу) компьютерной программы относительно того, что была нарушена тайна сообщений. Однако если с сервера оператора данных произошло разглашение тайны сообщений, то это уже совсем другая ситуация. Отсылая сообщения через сервер оператора данных, пользователь имеет право рассчитывать, что его данные останутся в тайне. С другой стороны, пользователь имеет право рассчитывать, что он в любой момент будет иметь возможность получить доступ к созданным им данным, находящимся на сервере оператора. То есть оператор данных должен позаботиться о конфиденциальности, целостности и доступности информации. В случае же, если были нарушены права пользователя как потребителя, пользователь может потребовать от разработчика программы возмещения вреда, наступившего в результате нарушения тайны передаваемых сообщений. Разработчик в таком случае в регрессном порядке может требовать возмещения от киберправонарушителя, нарушившего тайну сообщений.

Соглашение о пользовании компьютерной программой. По нашему мнению, положительной чертой законодательства в этой области было бы возложение на операторов больших данных обязанностей подробно объяснять пользователям процедуру дальнейшего использования данных, содержащихся в их сообщениях, а также отчитываться перед пользователями о выгодах, которые оператор получил в результате глубинной обработки таких данных. Следует четко запретить сканирование, прочтение содержания сообщений ПУПД. Не должно быть исключений, предлогов, под которыми оператор данных или принадлежащая ему компьютерная программа считывает содержание и конверт сообщения. Помимо этого, следует установить четкие законодательные запреты сбора данных, которые не являются необходимыми для работы скачиваемой, устанавливаемой компьютерной программы. Отказ приобретателя компьютерной программы согласиться с отдельными пунктами догово-

ра с владельцем, собственником компьютерной программы не должен быть основанием для отказа в предоставлении компьютерной программы. Перед пользователем не должен стоять несправедливый выбор: отказаться от тайны своих сообщений или отказаться от благ, которые предоставляет компьютерная программа. Наличие в договоре с пользователем подобных неравных условий, а также наличие в компьютерной программе скрытых, замаскированных, нечетко изложенных в прилагаемых документах функций, должно признаваться не только нарушением права на тайну сообщений, но и нарушением прав потребителя.

6.4. Правовой механизм защиты тайны сообщений пользователей услуг передачи данных от киберправонарушителей в Республике Беларусь: состояние и перспективы совершенствования

В Концепции информационной безопасности Республики Беларусь подчеркивается необходимость адаптации правовых норм, регулирующих право белорусских граждан на охрану тайны частной жизни, к развитию современных информационных технологий. Поэтому, на наш взгляд, разработка правового механизма обеспечения неприкосновенности частной жизни требует объединения усилий не только представителей юридического сообщества, но и специалистов в сфере информационных технологий. Именно в сотрудничестве правоведов с программистами и специалистами по защите информации видится перспективный путь, на котором можно добиться создания реальных гарантий этого важнейшего конституционного права белорусских граждан.

Право на тайну сообщений ПУПД закреплено в Республике Беларусь на конституционном уровне, а также в ряде законодательных актов. Законом установлена административная и уголовная ответственность за нарушение тайны сообщений пользователей, в том числе тех сообщений, которые передаются как электронные данные. Имеется также правовая база для применения технических и программных средств защиты информации. Для защиты информации о частной жизни, представляющей собой электронные сообщения, применение таких средств операторами компьютерных систем, сетей и ресурсов является обязательным. В Республике Беларусь действуют ряд международных правовых актов, нормы которых направлены на защиту права на тайну сообщений ПУПД.

В Республике Беларусь созданы и функционируют ряд органов, в обязанности которых входит защита от посягательств на тайну сообщений ПУПД. Это — Управление по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь, Следственный комитет Республики Беларусь, Управление безопасности в сфере информационных технологий Комитета государственной безопасности Республики Беларусь, Оперативно-аналитический центр при Президенте Республики Беларусь, Министерство связи и информатизации Республики Беларусь, Прокуратура Республики Беларусь. Существуют широкие возможности для су-

дебной защиты нарушенного права на тайну сообщений ПУПД в форме уголовного, административного, гражданского, конституционного судопроизводства. У белорусских пользователей услуг передачи данных есть возможности обратиться с жалобами о защите и (или) восстановлении своих прав на тайну сообщений к оператору услуг передачи данных, в государственные органы связи и информатизации, в правоохранительные органы.

Проанализированные в настоящей работе данные социологических исследований показывают, что при таком широком наборе правовых и институциональных инструментов случаи нарушения прав пользователей услуг передачи данных со стороны киберправонарушителей являются частыми, а сами пользователи не демонстрируют готовности воспользоваться имеющимся набором инструментов.

В ходе анализа правовых норм, анализа статистических данных, данных опросов, данных правоприменительной практики выявлены ряд факторов, которые снижают эффективность правового механизма защиты права на тайну сообщений ПУПД.

Это прежде всего чувство бессилия пользователей перед киберправонарушителями, убежденность в том, что единственным препятствием для взломов является защитное программное обеспечение. Однако пользователи смиряются с тем обстоятельством, что «если хакер захочет, то все равно взломает», поэтому отсутствует смысл в принятии строгих, разносторонних мер защиты. Такая система взглядов ведет к цифровому безразличию и несоблюдению цифровой гигиены.

Следующим фактором является отсутствие установки на восстановление своих нарушенных прав, непонимание целесообразности обращения в правоохранительные органы.

Следует отметить слабое освещение в белорусском информационном пространстве проблем ценности тайны частной жизни и персональных данных. В результате белорусские пользователи остаются безответственными по отношению к мерам личной цифровой безопасности.

Белорусским законодательством пока не установлены строгие требования к операторам персональных данных, которыми являются также и владельцы компьютерных программ, предназначенных для передачи сообщений. В ряде норм права устанавливаются лишь запреты на доступ к информации о частной жизни и персональным данным и на их разглашение. Однако не регламентирован вопрос разграничения случаев, в которых сбор информации является необходимым для функционирования компьютерной программы. Также законодательством не защищаются права человека на информацию, которая собирается с его согласия.

Для повышения мотивации пользователей защищать свои права, а также для повышения репутации правоохранительных органов целесообразно было бы предоставлять в открытый доступ информацию о результатах рассмотрения дел о нарушениях тайны сообщений ПУПД. Например, в СМИ была распространена информация о «пресечении осенью 2015 г. Комитетом государственной безопасности Республики Бела-

русь противоправной деятельность преступной группы, члены которой в течение трех лет прослушивали помещения и телефонные переговоры, а также взламывали электронную почту свыше двух тысяч белорусских граждан»[330]. Однако о завершении этих уголовных дел публике информация представлена не была.

Свою роль в повышении мотивации белорусских граждан защищать свое право на тайну сообщений ПУПД, а также в освещении проблем защиты данного права должна сыграть, прежде всего, наука. Необходимо увеличивать количество междисциплинарных правовых и IT-исследований о цифровых правах человека и стимулировать повышение их качества. Опубликование результатов таких работ даст понятные алгоритмы защиты прав.

По нашему мнению, многие из вышеперечисленных недостатков правового механизма защиты права на тайну сообщений ПУПД были бы, если не устранены, то, по крайней мере, сглажены в случае присоединения Республики Беларусь к таким основополагающим международным актам, как Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве) — Будапешт, 23 ноября 2001 года[331] и Конвенция «О защите физических лиц при автоматизированной обработке персональных данных»[332], а также в случае имплементации Руководства ОЭСР по защите неприкосновенности частной жизни и трансграничной передаче персональных данных[333].

Относительно защиты права на тайну сообщений пользователей услуг передачи данных от нарушений со стороны операторов данных проект Закона «О защите персональных данных» должен предусмотреть гарантии права субъекта на ознакомление со своими персональными данными. На данный момент проект закона не учитывает, что оператор может предоставить сведения о хранении, обработке не всех видов персональных данных. Гарантией права субъекта персональных данных мог бы стать запрет на обработку тех персональных данных, о которых субъект не был поставлен в известность. Также важно не ограничивать время применения мер по защите персональных данных моментом их обезли-

---

[330] *Сообщения о пресечении противоправной деятельности [Электронный ресурс] // Комитет государственной безопасности Республики Беларусь. Режим доступа : http://www.kgb.by/ru/news-ru/view/o-presechenii-protivopravnoj-dejatelnosti-112/. Дата доступа : 29.06.2019.*

[331] *Конвенция о компьютерных преступлениях : открыта к подписанию 23.11.2001 г. // Интернет-портал Совета Европы. Режим доступа : https://www.coe.int/ru/web/conventions/full-list/-/conventions/rms/0900001680081580. Дата доступа : 05.06.2019.*

[332] *Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера : открыта к подписанию 28 янв. 1981 г. // Интернет-портал Совета Европы. Режим доступа : https://www.coe.int/ru/web/conventions/full-list/-/conventions/rms/0900001680078c46. Дата доступа : 05.06.2019.*

[333] *Рекомендации Совета ОЭСР, касающиеся Руководства по защите неприкосновенности частной жизни и трансграничной передаче персональных данных 1980 г. (с изм. от 11 июля 2013 года) // Сайт ОЭСР [Электронный ресурс]. Режим доступа : https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf. Дата доступа : 29.08.2019.*

чивания. Такие меры должны приниматься до тех пор, пока существует техническая или иная возможность обработки данных, позволяющих идентифицировать физическое лицо.

Соглашение об использовании компьютерной программы должно содержать объяснения процессов обработки полученной от пользователя информации. В соглашении должно быть указано, для выполнения какой из функций компьютерной программы необходим сбор конкретного вида данных. Например, «доступ к журналу контактов устройства необходим компьютерной программе для совершения сеансов связи с данными контактами, с помощью данной программы». При подобной формулировке полностью бы исключалось использование данных журнала контактов, например для сбора статистической информации или для формирования баз данных текстов сообщений.

Заключение

Общая структура механизма правовой защиты тайны сообщений пользователей услуг передачи данных была обозначена уже на этапе проектирования исследования. Механизм включает все традиционно известные формы защиты исследуемого права: государственные (внесудебные и судебные), общественные и формы самозащиты. Последовательное выполнение задач исследования подтвердило гипотезу, согласно которой правовой механизм защиты права на тайну сообщений пользователей услуг передачи данных является несовершенным и нуждается в устранении дефектов. Одной из причин несовершенства данного правового механизма является разное осмысление процесса защиты тайны сообщений информатиками и юристами. Эта причина проявляется уже в отправных точках применения мер по защите информации — в том, что одни и те же вещи юристы и информатики называют разными словами. Эту проблему не решить простым переводом с юридического на IT-язык. Проблема решится только тогда, когда юристы и IT-специалисты будут исходить из общих теорий.

Дальнейший ход исследования показал недостаточность правового регулирования многих видов общественных отношений, связанных с обменом сообщениями между пользователями УПД. В то же время те нормы права, которые существуют в рассматриваемой области, часто не соответствуют ожиданиям пользователей УПД. На нерешенность данной проблемы существенно сказывается неимплементированность в белорусское законодательство некоторых норм международного права.

Среди таких проблем в области защиты права на тайну сообщений ПУПД необходимо отметить следующие. Это ограниченность защиты от кибервзломщиков лишь запретами и санкциями; практически полное отсутствие внимания законодателя к вопросам обработки больших данных; недостаточно четкие требования к поставщикам оборудования для сетей электросвязи; недостаточная правовая регламентация ответствен-

ности создателей компьютерных программ за их качество, в том числе за устойчивость программ к нарушению тайны сообщений ПУПД; недостаточная правовая защита пользователя компьютерной программы как слабой стороны лицензионного соглашения.

В связи с этим, по нашему мнению, совершенствование правового механизма защиты права пользователей услуг передачи данных на тайну сообщений должно происходить по следующим направлениям.

А) Совершенствование законодательства по защите права на тайну сообщений пользователей услуг передачи данных:

- закрепление в законодательном акте понятия сообщения, что позволит одновременно осуществлять защиту всех составных частей права на тайну сообщений пользователей услуг передачи данных: «*Сообщение — это электронные данные, передаваемые как совокупность знаков и символов, имеющие признаки начала и конца, представляющие собой единицу человеческого общения*»;
- включение в Уголовный кодекс (в главу 23) специальной нормы, устанавливающей ответственность за нарушение тайны сообщений пользователей услуг передачи данных;
- законодательное закрепление обязанности правоохранительного органа, оператора данных, которые выявили нарушение, информировать пользователя о нарушении тайны его сообщений. Это позволит пользователю предпринять меры по минимизации нанесенного ему вреда, а также своевременно начать процесс восстановления нарушенного права и возмещения вреда;
- в проекте Закона «О защите персональных данных» закрепление гарантий права субъекта на ознакомление со своими персональными данными, установить обязанность оператора данных информировать пользователя о том, что его данные в предусмотренных законом случаях предоставляться без его согласия;
- исходя из позиции, что персональные данные — категория нематериального характера, так как они неотделимы от личности носителя и подлежат защите в рамках такого объекта гражданских прав, как нематериальные блага, внести в п. 1 ст. 151 Гражданского кодекса Республики Беларусь изменения и дополнить перечень нематериальных благ персональными данными;
- с целью повышения уровня безопасности национального сегмента сети Интернет, определения надежности поставщиков оборудования для информационной инфраструктуры Беларуси внести дополнения в положения Указа Президента Республики Беларусь от 22 декабря 2014 г. № 612 по процедурам государственных закупок оборудования для реализации мероприятий программ информатизации;
- с целью повышения степени защищенности права на тайну сообщений пользователей услуг передачи данных принять меры по присоединению Республики Беларусь к Европейской Конвенции по киберпреступлениям, Конвенции «О защите физических лиц при автоматизированной обработке персональных данных».

Б) Совершенствование форм защиты права на тайну сообщений пользователей услуг передачи данных:

- разработать единую терминологию для обозначения субъектов и объектов информационных правоотношений с целью единообразного применения в нормативных правовых актах, правоприменительной документации, разрабатываемой производителями программных и аппаратных средств обработки информации;
- применить готовые алгоритмы выполнения позитивных обязанностей государства по защите права на тайну сообщений пользователей услуг передачи данных, которые содержатся в Руководстве ОЭСР по защите неприкосновенности частной жизни и трансграничной передаче персональных данных. Для Республики Беларусь актуальны такие содержащиеся в Руководстве предложения как «принятие закона, который бы обязывал распорядителей данных сообщать индивидам о взломе их систем», «принятие специального закона о защите неприкосновенности частной жизни», «создание специального органа, ответственного за защиту неприкосновенности частной жизни»;
- способствовать созданию независимого субъекта, уполномоченного рассматривать жалобы граждан о нарушении их права на тайну сообщений ПУПД и осуществлять защиту данного права граждан, что позволило бы упростить процедуру защиты права, минимизировать издержки этой процедуры для самого человека, повысить уровень мотивации граждан инициировать процедуру защиты своего права. ***Например, аналогично деятельности общества по защите прав потребителей.***

В) Проведение организационной работы по повышению возможностей человека пользоваться правом на тайну сообщений пользователей услуг электросвязи:

- значимой позитивной обязанностью государства могла бы стать обязанность предоставлять в открытый доступ информацию о результатах рассмотрения дел о нарушениях тайны сообщений ПУПД, а также обязанность правоохранительного органа, оператора данных, которые выявили нарушение, информировать пользователя о нарушении тайны его сообщений.

Считаем необходимым продолжить исследования, касающиеся совершенствования правового механизма защиты права на тайну сообщений ПУПД, поскольку каждое из направлений совершенствования требует глубокой научной подготовки.