

ПРАВОВАЯ ОХРАНА СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

А.А. Игнатъев, магистрант

Северо-Восточный федеральный университет им. М.К. Аммосова
(Россия, г. Якутск)

DOI:10.24412/2500-1000-2022-3-1-147-152

***Аннотация.** Обеспечение информационной безопасности в современном мире является одним из самых сложным и специфическим процессом, который подвержен воздействию множества внешних и внутренних факторов. Среди информации особую ценность представляют сведения конфиденциального характера. Информационная безопасность должна обеспечиваться не только техническими, программными и организационными средствами, но также и законодательными, в целях регламентации правил использования, обработки, передачи информации и других действий, установления полномочий, а также мер ответственности за нарушение предписанных правил. В связи с этим сформировался в российском праве такой институт как – институт защиты сведений конфиденциального характера.*

Учитывая вышеизложенное, в настоящей статье автором будет рассмотрен вопрос о том, насколько российское законодательство в части защиты сведений конфиденциального характера соответствует эпохе времени.

***Ключевые слова:** сведения конфиденциального характера, персональные данные, информация, информационная безопасность, законодательство, правоприменение, ответственность.*

Актуальность исследования выражена в том, что информация в настоящей информационной эпохе является одним из главных ресурсов общественного развития и ее ценность растет с высокой скоростью. С развитием информационных отношений стали появляться средства, методы обработки информации и другие цифровые технологии, которые все более стали проникать в жизнь современного общества.

Нельзя не согласиться с утверждением о том, что право должно идти в ногу со временем. Действительно, за последнюю пару десятков лет российское законодательство претерпело достаточно много изменений в области цифровых технологий. При этом не стоит придавать феномену цифровизации права статуса панацеи от всех бед российской правовой действительности и многих социальных проблем. Цифровизацию следует рассматривать лишь как один из дополнительных способов оптимизации правового регулирования при помощи цифровых технологий.

Обеспечение информационной безопасности в современном мире является одним из самых сложным и специфическим про-

цессом, который подвержен воздействию множества внешних и внутренних факторов. Информационная безопасность должна обеспечиваться не только техническими, программными и организационными средствами, но также и законодательными, в целях регламентации правил использования, обработки, передачи информации и других действий, установления полномочий, а также мер ответственности за нарушение предписанных правил. В связи с этим сформировался в российском праве такой институт как – институт защиты информации.

Учитывая вышеизложенное, в настоящей статье будет рассмотрен вопрос о том, насколько российское законодательство в части защиты сведений конфиденциального характера соответствует эпохе времени.

Цифровизация уголовного процесса предполагает раскрытие термина «информация». Несмотря на то, что в современном мире человек постоянно имеет дело с информацией, строгого научного определения, что же такое информация, не существует. В литературе можно найти огромное множество определений термина «ин-

формация», которые содержат различные подходы к толкованию данного определения [9].

В современном обществе информация является ценным ресурсом, нуждающемся в надежной защите. Объектом защиты является информация или носитель, на котором содержится информация, или различные информационные процессы, нуждающиеся в защите в соответствии с поставленными целями. Из-за огромного разнообразия видов носителей информации, а также из-за возможности перехода информации из одной формы в другую не представляется возможным определить полный перечень объектов информации, подлежащих защите.

Современное информационное общество использует в своей деятельности довольно широко компьютерные технологии, телекоммуникационные сети, электронные библиотеки, базы данных, автоматизированные системы, системы искусственного интеллекта и многое другое. Использование различных автоматизированных систем обработки информации и управления послужило фактором обострения защиты информации от несанкционированного доступа [14].

В связи с этим главной и актуальной проблемой двадцать первого века, являющегося эпохой развития технологий и информатизации всех сфер жизнедеятельности современного общества, становится проблема обеспечения информационной безопасности.

Интенсивное развитие автоматизированных технологий в сфере распространения, обработки и передачи информации, внедрение их во все социальные сферы жизнедеятельности российского общества повышают уязвимость частной жизни граждан, создают очевидные угрозы незаконного оборота персональных данных, в том числе и конфиденциальные данные.

Необходимо рассматривать и сравнивать конфиденциальные сведения в двух аспектах:

1) конфиденциальные сведения как объект защиты уголовного законодательства;

2) конфиденциальные сведения как объект защиты уголовно-процессуального законодательства.

Данное разделение обусловлено принципиальными отличиями самого объекта, разными составами правовых отношений, методами и способами их регулирования.

Конфиденциальность информации – это необходимость предотвращения несанкционированного доступа к ней со стороны третьих лиц. Конфиденциальная информация – это любые данные, которые не подлежат огласке.

На сегодняшний день действует Перечень сведений конфиденциального характера, утвержденный Указом Президента РФ от 06.03.1997 г. № 188, к которым относятся [8]:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

- сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц;

- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.);

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

- сведения о сущности изобретения, полезной модели или промышленного образ-

ца до официальной публикации информации о них;

- сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными.

Другим нормативным актом, устанавливающим виды информации с ограниченным доступом, является Федеральный закон «Об информации, информационных технологиях и о защите информации», ст. 9 которого содержит следующий перечень конфиденциальных сведений: государственная, коммерческая, служебная, профессиональная тайны, информация о частной жизни гражданина и персональные данные.

Следует отметить, что в указанные перечни не вошли такие широко используемые сегодня (и имеющие правовую регламентацию) виды тайн как тайна усыновления, банковская, налоговая и прочие тайны. Как оценивают некоторые авторы, действующее законодательство насчитывает более 30 видов различных тайн.

Необходимо отметить, что, основываясь на основных принципах права, таких как демократизм, гуманизм, справедливость, персональные данные человека и гражданина следует признавать наиболее ценными среди других видов конфиденциальной информации. Соответственно, защита правовых отношений в этом направлении должна соответствовать эквиваленту ценности охраняемых объектов.

В настоящее время уровень информационных технологий настолько высок, что уже не представляется возможным говорить о самозащите прав в сфере информационных технологий, поскольку это является не эффективным способом борьбы с посягательствами на частную жизнь. Необходимость в принятии мер по защите информации, составляющей сведения о человеке, обусловлена ростом технических возможностей потенциального злоумышленника по несанкционированному доступу, копированию, модификации, блокированию и уничтожению информации.

При защите любого вида информации необходим комплексный подход, который предполагает, в том числе, и правовые методы защиты. Именно поэтому в Российской Федерации создана нормативно-правовая база по защите сведений конфиденциального характера.

Как отмечает М.А. Ефремова, «проблемой является тот факт, что на сегодняшний день нет легального определения термина «информация» для целей уголовного права, хотя уголовный закон им оперирует», «предметом уголовно-правовой охраны является не вся совокупность информации, а только обладающая установленными признаками. Правоприменитель сталкивается с проблемами отсутствия ее точных признаков либо их недостаточной проработанностью для использования» [12].

Основной характеристикой движения информации является технологическая комплексность, а также защищенность. Порядок и маршруты потоков конфиденциальных документов на бумажном носителе и электронных документов в инфраструктуре организации, включая информационную инфраструктуру организации, должны быть документированы и регламентированы для того, чтобы процесс восстановления работоспособности системы документооборота, включая электронный, производился максимально быстро.

Таким образом, помимо персональных данных, к перечню конфиденциальных относятся и другие виды информации. Они утверждены законом «О перечне сведений конфиденциального характера».

Тайна следствия и данные о ходе судопроизводства. Федеральные законы «О защите судей, должностных лиц правоохранительных органов», «О защите потерпевших, свидетелей и других участников судопроизводства» утверждают конфиденциальность данных в отношении лиц, участвующих в расследовании уголовных дел.

Служебные сведения. Доступ к ним ограничен Гражданским кодексом нашей страны. Информация такого характера является служебной тайной и не может быть распространена без согласия обладателя.

Врачебная / нотариальная / адвокатская тайна. Доступ к таким данным ограничивается Конституцией государства. Не могут быть распространены переписки, записи телефонных переговоров, почтовые отправления и другое, если они выступали каналом коммуникации между обладателем информации и лицом с обязанностями хранить профессиональную тайну в сфере общения со своим клиентом.

Коммерческая тайна (ограничено Гражданским кодексом РФ). Сведения об изобретениях, полезных моделях и промышленных образцах.

За разглашение информации и распространение документов, содержащих конфиденциальную информацию, гражданин может быть привлечен к дисциплинарной, материальной, административной и уголовной ответственности в зависимости от тяжести проступка. Распространение данных, доступ к которым был ограничен федеральным законом, влечет за собой административную ответственность (статья 13.14 Кодекса РФ об административных правонарушениях [2]).

Гражданину в Российской Федерации придется заплатить штраф в размере от 500 до 1000 рублей, штраф для должностных лиц, включая адвокатов, возрастает до 5000 рублей.

За разглашение коммерческой, служебной или государственной тайны работнику предприятия будет грозить дисциплинарная ответственность, предусмотренная статьями 57, 81, 192 и 193 Трудового Кодекса РФ [3]. Предусмотрены дисциплинарные взыскания: Замечание. Выговор. Увольнение (По статье 81 ТК РФ «Расторжение договора по инициативе работодателя»). Если распространение информации нанесло вред предприятию, наступает материальная ответственность. Статьи 232 и 238 предусматривают возмещение потерь в полном объеме. Если разглашение конфиденциальных данных привело к материальному ущербу, то пострадавшая сторона может потребовать компенсацию в судебном порядке.

За выдачу сведений под грифом «государственная тайна» иностранному государству, организации или гражданину

предусмотрено наступление уголовной ответственности.

Согласно статьям 283, 284 и 275 Уголовного Кодекса РФ [4] за данное деяние предусмотрено следующее наказание – лишение свободы сроком от 12 месяцев до двадцати лет в зависимости от обстоятельств, а согласно статье 284 УК РФ (Утрата документов, содержащих государственную тайну) дополнительно накладывается штраф в размере до 500 000 рублей или заработной платы в период до 3 лет. Законодательство Российской Федерации защищает конфиденциальность информации, а граждане, столкнувшиеся с нарушениями, могут отстаивать свои права и получить компенсацию.

Для того чтобы выявить факт совершения нарушения в области защиты информации необходимо наличие определенных действий, посягающих на безопасность информации, это может быть как несанкционированный доступ, несоблюдение требований законодательства, распространение, не предоставление информации, копирование, уничтожение, модификация, блокирование и другие действия. На выявление и квалификацию правонарушений в информационной сфере большое влияние оказывает состояние информационной среды субъекта, чьи права и интересы нарушаются.

На практике, мы становимся очевидцами многочисленных массовых «сливов» охраняемых сведений, но не слышим новостей о поимке злоумышленников. Данное обстоятельство свидетельствует о том, что основной проблемой защиты сведений конфиденциального характера является правоприменение, то есть механизм по выявлению и расследованию фактов неправомерного разглашения сведений информационного характера.

Полагаю необходимым усилить защиту персональных данных в правоприменительной области путем методологического исследования тактики выявления и расследования фактов неправомерного разглашения охраняемых сведений ради снижения возможности использования данной информации в незаконных целях. Несмотря на приличный базис законодательства,

посвященного проблеме защиты персональных данных, и достаточность на первый взгляд способов защиты, предлагаемых гражданским и уголовным законодательством для защиты гражданина в случае ответственного подхода к выполнению требований законодательства, усиление,

развитие данной сферы только улучшит общественные отношения в целом.

Таким образом, действующее законодательство в области охраны сведений конфиденциального характера формально соответствует духу времени, однако уровень практического применения мер по охране таких сведений объективно не высокий.

Библиографический список

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Собрание законодательства Российской Федерации. – 2020. – № 31. – Ст. 4398.
2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 30.12.2021) (с изм. и доп., вступ. в силу с 01.02.2022) // Собрание законодательства Российской Федерации. – 2001. – № 34. – Ст. 3077.
3. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 22.11.2021) (с изм. и доп., вступ. в силу с 30.11.2021) // Собрание законодательства Российской Федерации. – 2001. – № 34. – Ст. 1806.
4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 30.12.2021) // Собрание законодательства Российской Федерации. – 1996. – №25. – Ст. 2954.
5. Закон РФ от 21.07.1993 № 5485-1 (ред. от 11.06.2021) «О государственной тайне» // Собрание законодательства Российской Федерации. – 1997. – № 41. – Ст. 4673.
6. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 30.12.2021) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2022) // Собрание законодательства Российской Федерации. – 2006. – №31 (ч.1). – Ст. 3448.
7. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 02.07.2021) «О персональных данных» // Собрание законодательства Российской Федерации. – 2006. – №31 (ч.1-2). – Ст. 3451.
8. Указ Президента Российской Федерации от 06.03.1997 г. № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера» // Собрание законодательства Российской Федерации. – 1997. – №10, – ст. 1127.
9. Багмет А.М. Сохранение в тайне персональных данных участников уголовного судопроизводства / А.М. Багмет, Н.В. Османова // Российский судья. – 2019. – №7. – С. 27-33.
10. Голованова Н.А. Уголовно-юрисдикционная деятельность в условиях цифровизации: монография. – М.: ИЗиСП, КОНТРАКТ, 2019. – 212 с.
11. Гутник С.И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных: дисс. ... канд. юрид. наук. – Хабаровск, 2017. – 241 с.
12. Ефремова М.А. Социальная обусловленность уголовно-правовой охраны информационной безопасности Российской Федерации // Вестник Пермского университета. Юридические науки. – 2017. – №2. – С. 222-230.
13. Лавриненко А.В. К вопросу о проблеме использования персональных данных в электронном правосудии / А.В. Лавриненко, Д.А.-А. Суюмбаева // Электронное правосудие и процессы цифровизации права: проблемы и перспективы. Материалы III Международного научно-практического конвента студентов и аспирантов / сост. Ю.М. Лукин. – Казань: Изд-во Казанского ун-та, 2018. – 312 с.
14. Лопатин В.Н. Информационная безопасность в электронном государстве // Информационное право. – 2018. – №2. – С. 14-19.

LEGAL PROTECTION OF CONFIDENTIAL INFORMATION

A.A. Ignatiev, *Graduate Student*

North-Eastern Federal University named after M.K. Ammosova

(Russia, Yakutsk)

***Abstract.** Ensuring information security in the modern world is one of the most complex and specific processes that is influenced by many external and internal factors. Information of a confidential nature is of particular value. Information security should be ensured not only by technical, software and organizational means, but also by legislative ones, in order to regulate the rules for using, processing, transferring information and other actions, establishing powers, as well as measures of responsibility for violation of the prescribed rules. In this regard, such an institution as the Institute for the Protection of Confidential Information has been formed in Russian law. Considering the foregoing, in this article the author will consider the question of how Russian legislation in terms of protecting confidential information corresponds to the era of time.*

***Keywords:** confidential information, personal data, information, information security, legislation, law enforcement, responsibility.*