УДК 34.096

ИНФОРМАЦИОННЫЕ СПОСОБЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ЛИЦ В АСПЕКТЕ ПРОТИВОДЕЙСТВИЯ КОРРУПЦИИ*

Каюшникова Ю. Е., старший преподаватель кафедры конституционного
и административного права
Волгоградский институт управления – филиал РАНХиГС, г. Волгоград

Аннотация. В статье анализируются отдельные способы защиты персональных данных лиц, предоставляющих сведения о доходах, расходах, имуществе и обязательствах имущественного характера в аспекте противодействия коррупции.
Ключевые слова: информация, персональные данные, противодействие коррупции, сведения о доходах, право на забвение.

INFORMATION METHODS OF PROTECTING PERSONAL DATA OF PERSONS IN THE ASPECT OF COMBATING CORRUPTION

Kayushnikova Yu. E., Senior Lecturer, Department of Constitutional and Administrative Law
Volgograd Institute of Management – branch of RANEPA, Volgograd

Abstract. The article analyzes certain methods of protecting personal data of persons providing information on income, expenses, property and property obligations in the aspect of combating corruption.
Keywords: information, personal data, anti-corruption, information about income, the right to be forgotten.

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, в том числе и к сведениям, которые публикуются на сайтах органов исполнительной власти в соответствии с необходимостью предоставлять сведения о доходах, расходах, иму-

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16119 «Формирование антикоррупционной среды в органе государственной и муниципальной власти путем внедрения информационно-аналитической системы «Методика и тактика противодействия коррупции для государственных и муниципальных служащих».

ществе и обязательствах имущественного характера (далее также – сведения о доходах) и обнародовать их в соответствии с принципом транспарантной государственной и муниципальной службы.

В связи с этим главной и актуальной проблемой двадцать первого века, являющегося эпохой развития технологий и информатизации всех сфер жизнедеятельности современного общества, становится проблема системной обеспеченности безопасности персональных данных в целом и данных о лицах, предоставляющих сведения о доходах, в частности.

Появление подкласса персональных данных из класса частной жизни, связывается с повсеместным распространением распределенных автоматизированных информационных систем, а также баз данных, обеспечивающих хранение и обработку информации. Чаще всего доступ к таким системам организован с помощью компьютерных сетей, что дает возможность потенциальному злоумышленнику получить удаленный доступ к системе.

Также важность защиты данных, составляющих сведения о человеке, определяется возможностью неправомерного к ним доступа со стороны злоумышленника, в результате чего полученные им сведения превратятся в орудие и средство совершения преступления. Например, хищение из баз данных антропометрических характеристик человека может привести к несанкционированному доступу к какой-либо автоматизированной информационной системе с биометрической аутентификацией. Таким образом, произойдёт компрометация действий пользователя, чьи данные были украдены, для входа в систему. Это актуально для баз данных Росреестра, например. Злоумышленники получают достаточно подробную информацию об имуществе служащего (его супруга или несовершеннолетнего ребенка) и могут в дальнейшем использовать ее в противоправных целях.

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 [2].

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 персональных данных.

Персональные данные нуждаются в комплексном подходе к обеспечению состояния их защищенности. Для этого нужна отлаженная система нормативно-правовых документов, регламентирующих порядок обработки, хранения, передачи и защиты персональных данных.

Оператором является государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки

персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Оператор также может назначить лицо, которое будет ответственно за обработку персональных данных.

Также существуют технические меры обеспечения безопасности персональных данных, которые устраняют оставшиеся угрозы, посредством установки программных или аппаратных средств защиты информации (межсетевые экраны, антивирусы, IDS и т.д.). Полный перечень мер необходимых для защиты информационных систем, обрабатывающих персональные данные, представлен в приказе ФСТЭК № 21 от 18 февраля 2013 г.

Говоря о мерах защиты персональных данных, важно отметить, что обработка данных осуществятся только с наличия согласия субъекта, чьи персональные данные подлежат обработке. Обработка данных нужна для исполнения договора, одной из сторон которого является субъект персональных данных.

Персональные данные лиц, предоставляющих сведения о доходах, следует отнести к двум категориям: биометрические и иные.

Говоря о защите персональных данных лиц, предоставляющих сведения о доходах, очень важно отметить тот факт, что передача таких персональных данных третьим лицам не допускается без письменного согласия самого служащего. Однако в данном случае предусмотрены определенные исключения. Например, согласие государственного служащего не требуется при передаче его данных, если это связано с выполнением им должностных обязанностей, в том числе при командировании.

Согласие служащего также не требуется в случае мотивированных запросов от органов прокуратуры, правоохранительных органов, органов безопасности, от государственных инспекторов труда при осуществлении ими государственного надзора за соблюдение трудового законодательства, а также иных органов, которые уполномочены запрашивать информацию о работниках [1].

Важно отметить тот факт, что передача персональных данных государственных служащих кредитным организациям, которые открывают счета и обслуживают платежные карты для начисления заработной платы, не требует согласия самих служащих в том случае, если договор на выпуск банковских карт заключался с представителем нанимателем. Но главное, чтобы в тексте договора были предусмотрены положения о передаче представителем нанимателем персональных данных госслужащих.

Персональные данные содержат в себе сведения о человеке, такая информация всегда имела большую значимость, а в современном мире являются одним из самых дорогих товаров.

Важность защиты персональных данных продиктована возможностью неправомерного доступа к ним со стороны злоумышленника, в конечном счете, полученные им сведения превратятся в орудие и средство совершения преступления.

Персональные данные государственных служащих также могут стать способом совершения преступления. Например, если важные данные окажутся в руках злоумышленника, то они могут стать товаром для продажи третьим лицам.

Лица, обеспечивающие защиту персональных данных, в случае не надежной защиты, приведшей в итоге к неправомерному доступу к информации, несут ответственность. Существует несколько видов ответственности. В случае нарушения закона о персональных данных может наступить административная, уголовная, гражданско-правовая, дисциплинарная ответственности.

Исследуя тему персональных данных нельзя не отметить, что законодательно закреплено право на забвение, иначе говоря, право быть забытыми. Изначально право на забвение было принято Европейским судом после издания постановления, которое обязало Google удалять неточную, заведомо ложную и больше неактуальную информацию о человеке по его запросу. Основанием для принятия законопроекта послужило дело испанца Марио Гносалеса против GoogleSpain. Гносалес обнаружил, что в поисковой строке Google по его имени выдается старая информация о судебных извещениях имевших двадцатилетнюю давность и об аукционе из-за долгов, а также об аресте дома, которая содержалась в одной из испанских газет. Тогда он обратился в Google с требованием скрыть его персональные данные в результате поиска и удалить ссылку на сайт, где содержится неактуальная информация.

Судебное разбирательство длилось пять лет и вынесенное в итоге решение было в пользу испанца. Таким образом, появилось право на забвение, которое представляет собой удаление информации по просьбе заявителя.

При этом на сегодняшний день ни один нормативно-правовой акт, к сожалению, не предусматривает такого права на забвение для государственных служащих и иных лиц, предоставляющих сведения о доходах.

Угрозы информации в сфере защиты открытых данных о лицах, выполняющих свои антикоррупционные обязательства, следует классифицировать по следующим признакам:

1. По природе возникновения: естественные угрозы (они связаны с природными процессами) и искусственные угрозы (возникают из деятельности человека).

2. По источникам возникновения угроз: природная среда, человек, санкционированные программно-аппаратные средства, несанкционированные программно-аппаратные средства.

3. По зависимости от активности системы: проявляются только в процессе обработки данных или в любое время.

4. По способу доступа к ресурсам: стандартные угрозы и нестандартные угрозы.

5. По месту расположения информации: внешние носители, оперативная память, линии связи, устройства ввода-вывода.

Для должного уровня обеспечения информационной безопасности необходимо использовать такие средства защиты информации от угроз как: формальные, аппаратные, физические, криптографические, программные, организационные, законодательные и морально-этические. Однако, использование только средств защиты информации недостаточно для обеспечения информационной безопасности. Должное внимание в этом вопросе необходимо уделить законодательству, составляющему основу института защиты информации. Необходимо улуч-

шение понятийного аппарата на законодательном уровне, более подробная и четкая регламентация и закрепление определенных положений, а также устранение противоречий между законодательными актами, которые можно встретить при изучении нормативно-правовой базы.

Итак, важным этапом в обеспечении защиты частной жизни является защита персональных данных.

В случае нарушения закона о персональных данных может наступить административная, уголовная, гражданско-правовая, дисциплинарная ответственности. Чаще всего ответственность является административной в виде предупреждения или штрафа. У субъектов персональных данных, есть право на забвение, которым они могут воспользоваться в случае, если информация о них является недостоверной или неактуальной.

Сегодня защита информационных систем от выше перечисленных проблем требует возрастания роли программных, криптографических механизмов, а также использования протоколов, механизмов с высокой вычислительной сложностью. Однако, отсутствие достаточного количества средств защиты информации и технического оснащения в органах исполнительной власти еще долгое время не позволит осуществлять мероприятия по защите данных о лицах, предоставляющих сведения о доходах, расходах, имуществе и обязательствах имущественного характера в необходимых масштабах

Для того, чтобы обеспечить должный уровень информационной безопасности необходимо минимизировать случаи столкновения с проблемами, которые рассмотрены в данной статье, повысить уровень информационной грамотности, повышать уровень подготовки специалистов в области защиты информации, обеспечить каждый орган власти необходимыми средствами защиты, техническим оборудованием. Также необходимо стремиться к обеспечению единства, устойчивости и безопасности информационной инфраструктуры Российской Федерации на всех уровнях информационного пространства.

Библиографический список

1. Астафурова О. А., Голоманчук Э. В., Меграбян Д. А. Современные способы осуществления коррупции на государственной гражданской службе и способы противодействия им // Бизнес. Образование. Право. 2020. № 3 (52). С. 309-316. DOI: 10.25683/VOLBI.2020.52.378.

2. Голоманчук Э. В. Отдельные возможности внедрения и использования информационно-коммуникационных технологий в системе противодействия коррупции // Проблемы противодействия коррупции в современном обществе [материалы] (2020; Волгоград) / под ред. Э. В. Голоманчук; Волгоградский институт управления – филиал ФГБОУ ВО «Российская академия народного хозяйства и государственной службы». Волгоград: редакционно-издательский отдел ГБПОУ «Волгоградский технологический колледж», 2020. (РИНЦ). С. 42-45.