БЕЗОПАСНОСТЬ ЛИЧНЫХ ДАННЫХ ВО ВСЕМИРНОЙ ИНФОРМАЦИОННОЙ СЕТИ

SECURITY OF PERSONAL DATA IN THE WORLD WIDE WEB INFORMATION NETWORK

УДК 004.056

Пиджикян Диана Сергеевна, студент 2 курса, факультет «Управления», Южно-Российский институт управления РАНХиГС при Президенте Российской Федерации, Россия, г. Ростов-на-Дону

Научный руководитель: Хашева Ирина Анатольевна

Pijikyan D. S., pijikyan.diana777@gmail.com

Scientific adviser: Khasheva Irina Anatolyevna

Аннотация

В данной статье рассматривается один из ключевых вопросов, посвященных информационной безопасности личности. В работе раскрыто место и роль нормативно-правого регулирования данной сферы, освещены законодательные проблемы в Российской Федерации, а также разработана система рекомендаций по обеспечению гражданами безопасности личных данных в сети Интернет.

Abstract

This article discusses one of the key issues related to personal information security. The paper reveals the place and role of legal regulation in this area, highlights the legislative problems in the Russian Federation, and also develops a system of recommendations for ensuring the security of personal data on the Internet by citizens.

Ключевые слова: Интернет, конфиденциальность, безопасность личных данных, защита информации, мошенники.

Keywords: Internet, privacy, personal data security, information protection, scammers.

В современном информационном обществе, нельзя представить свою жизнь без интернета. Разные приложения, социальные сети, сайты и поисковые системы постоянно собирают информацию о пользователях. Эти данные нужны для анализа интересов посетителей страниц, настроек рекламы и изучения целевой аудитории. Однако появление и распространение информационных технологий не только значительно упростило жизнь современного общества, но и повысило шансы стать жертвой информационной атаки на личные данные.

Данная проблема стала очевидной еще в прошлом столетии на этапе становления информационных взаимоотношений. Поэтому с целью регулирования этой сферы жизни общества, а также защиты интересов населения, начала формироваться нормативно-правовая база по предупреждению информационных правонарушений и похищения данных.

Так, фундаментальной основой для становления современной системы нормативно-правовых актов в сфере информационной безопасности Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера, подписанная еще в 1981 году [2]. Данный документ закреплял ряд основополагающих принципов по обработке персональных данных:

- персональные данные могут использоваться только для личных целей и до истечения конкретного срока, зависящего от цели добавления информации и степени ее важности;
- актуальность персональных данных в связи с постоянным обновлением и пользованием ими;
- обладатель персональных данных, на время попавших в базу данных, обеспечивается гарантированными правами и др.

Некоторые из них не утеряли свою актуальность и по сей день и нашли свое отражение в современном Федеральном законе от 27.07.2006 №152-ФЗ "О персональных данных" (рис. 1)

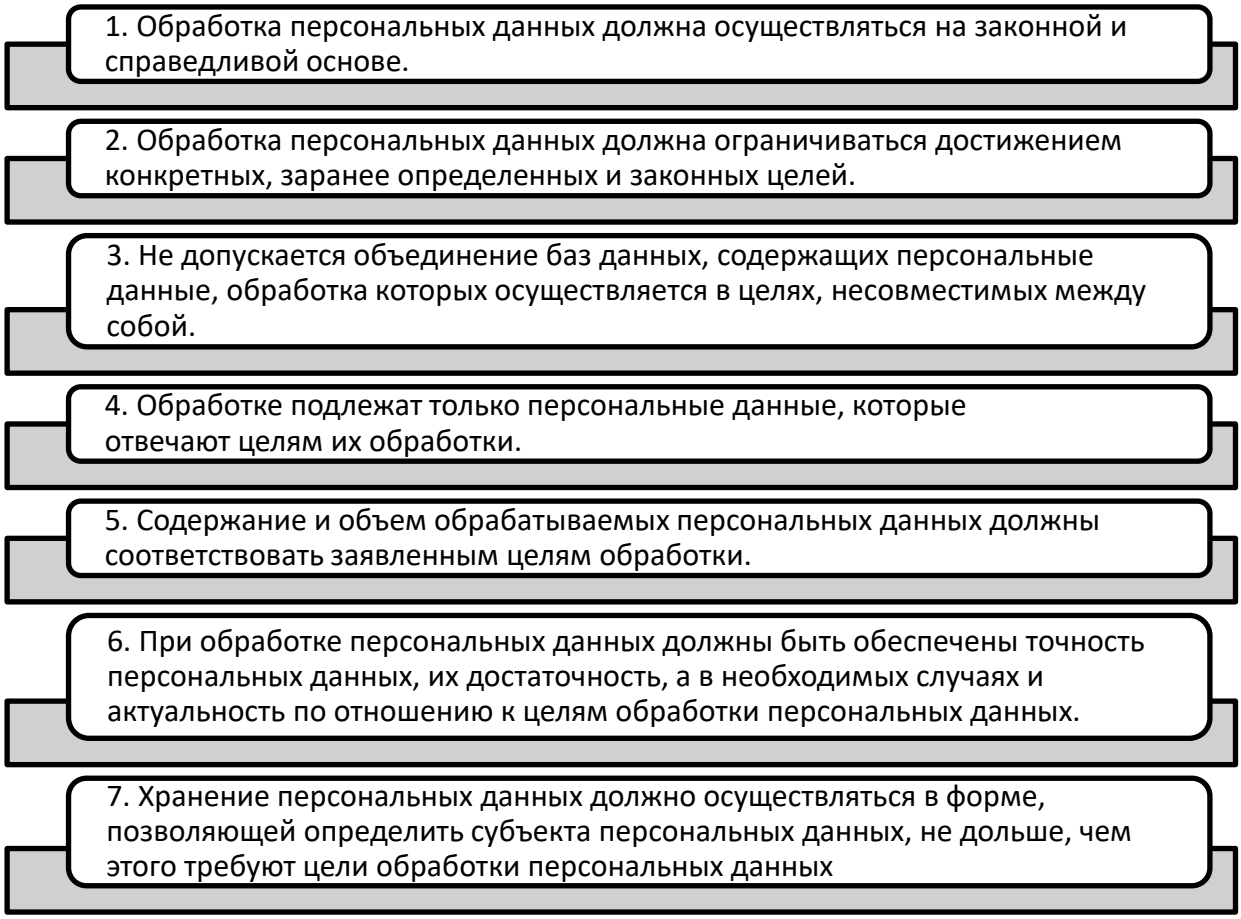

Рис. 1. Принципы обработки персональных данных [1].

Сегодня в век развития цифрового пространства мировое сообщество уделяет особое внимание информационной безопасности. Говоря о международном сотрудничестве, отметим, что в рамках активной работы по защите персональных данных, в 2018 году Россия приняла участие в подписании Протокола о внесении изменений в Конвенцию Совета Европы. На основе данного документ граждане теперь могут в любой момент получить консультацию или юридическую помощь, связанную с вопросами передачи, хранения и изменения личной информации. Кроме того, российские предприятия, чья деятельность должна соответствовать требованиям Совета Европы, избавлены от необходимости обеспечивать данные своих потребителей

дополнительной защитой, так как все меры защиты персональной информации должны обеспечиваться исполнительными органами Совета Европы.

Несмотря на то, что сегодня государством обеспечивается нормативно-правовое регулирование данного вопроса, личная безопасность в сети Интернет зависит от самого себя и своих действий, поскольку с одной стороны, при регистрации, входе в определенный аккаунт, браузер предлагает запомнить пароль с логином, чтобы в следующий раз человеку не пришлось тратить время на поиск и ввод своих секретных данных. С другой, потакание такому удобству зачастую является причиной совершения информационных правонарушений, кражи персональных данных, использования их в своих целях и т.д. В связи с этим представляется необходимым рассмотреть некоторые основы обеспечения личной информационной безопасности при использовании сети Интернет.

Для того, чтобы сохранить данные, но при этом не переживать за их распространение, необходимо реализовать комплекс мероприятий. Сохранность паролей от социальных сетей, мессенджеров, электронной почты и прочего являются важнейшим аспектом в данном вопросе. В первую очередь следует понимать, что хранение информации о паролях на компьютере, который используется для выхода в интернет является не целесообразным. Ошибкой также станет использование информации для пароля, которая находится в открытом доступе, например, дата рождения. Применение двухэтапной аутентификацией, сложные пароли длиной не менее 8 символов с использованием заглавных и строчных букв, цифр, специальных значков %$#, а также частая их замена - есть залог надёжной защиты аккаунтов. Чтобы не оказаться в невыгодной ситуации, необходимо тщательно изучать политику конфиденциальности сайта или приложения, которую многие зачастую пропускают. На наш взгляд необходтмо убедиться, что сайт или приложение не получает права распоряжаться вашими личными данными и передавать третьи лицам.

Для гарантии информационной безопасности также серьезным условием является верно настроенный браузер. Специалисты в сфере IT-индустрии

рекомендуют держать в отключенном виде опцию «автоматически запоминать пароли», особенно для сайтов, где нужно вводить номер банковской карты или номера документов. Отдельное внимание стоит уделить геолокации и чистке cookies. Геолокация передает данные о местоположении пользователя, но это далеко не единственная функция геолокаций. Помимо местоположения, геолокация передает такие данные, как фотоснимки, заметки пользователя, маршрут и т.д. В связи с этим, если на данный момент пользователь не нуждается в определении местоположения или построении маршрута, то геолокацию лучше отключать.

Файлы cookies – это файлы Интернета, которые переносят в себе информацию о тех сайтах, которые посещает пользователь во время пользования Интернетом. Благодаря этим файлам, очень сильно упрощается жизнь: все интересы и предпочтения, любимые сайты, закладки, тематики статей и т.д. – все это хранится и затем пользователю не нужно вводить все желаемое в очередной раз. Однако все, что полезно, еще и опасно. Поэтому необходимо регулярно чистить подобные файлы, проверять их на наличие какой-либо персональной информации и т.д.

Вышеизложенное это далеко не полный перечень возможных мер, по обеспечению безопасности личных данных, однако сказанное позволяет сделать вывод о том, что сегодня несмотря на разработанные меры со стороны государства, личность остается достаточно уязвимой с точки зрения информационной сохранности. Данный вывод подкрепляется и рядом прецедентов по утечке личных данных населения.

Так, например, в 2019 году Forbes сообщил, что исследователи обнаружили на незащищенном сервере почти 2 млрд. пользовательских записей «Умного дома» китайской компании Orvibo, которые содержали различную информацию – от кодов сброса учетных записей до паролей пользователей.

В свою очередь, в этот же год на портале KrebsonSecurity опубликовали статью, из которой стало известно, что крупная американская страховая компания First American Financial Corporation допустила утечку 885 млн.

оцифрованных данных клиентов: банковские реквизиты, номера социального страхования, квитанции о транзакциях, изображения водительских прав и пр.

Что касается российского опыта, отметим, что достоянием общественности стал инцидент, связанный с тем, что Бобом Дьяченко в сотрудничестве со специалистами портала Comparitech.com была обнаружена база с 20 млн. налоговых деклараций граждан России за период с 2009 по 2016 год, которая была доступна без пароля на сервере Amazon Web Services Elasticsearch. Записи включали в себя ФИО, адреса, статусы резидентов, номера паспортов, телефонные номера, идентификационные номера налогоплательщиков, имена работодателей и суммы налогов. Данное является абсолютно недопустимым и, по нашему мнению, предпосылкой для таких действий могло стать несовершенство федерального законодательства.

На сегодняшний день в России разобраться в нюансах обработки персональных данных бывает не просто даже опытным специалистам. Это связано с тем, что положения Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" содержат общие формулировки, которые могут трактоваться по-разному. Позиции Роскомнадзора и суда по одному и тому же вопросу могут различаться, более того, встречаются судебные дела с противоположными решениями. При построении процессов обработки персональных данных руководители компаний часто не понимают, на что им ориентироваться, чтобы не допустить нарушений закона.

При этом вопрос защиты персональных данных год от года становится более острым. За последние два года в КоАП РФ внесены поправки об увеличении штрафов за невыполнение требований нормативно-правового акта. Кроме того, сейчас готовится проект закона об увеличении штрафов за утечку персональных данных. Ежегодно Роскомнадздор фиксирует более 50 тыс. жалоб физических лиц и выписывает организациям административные штрафы, общая сумма которых превышает 1 млн руб. Возможные последствия для компаний не ограничиваются одними штрафами: регулятор может заблокировать сайт

организации, что является неотъемлемой частью бизнеса для тех, кто предоставляет онлайн-сервисы или развивает продажи в интернете.

Таким образом, статистика показывает, что утечка данных является актуальной проблемой для любой организации. Имеющаяся сегодня законодательная база позволяет регулировать вопросы данной сфере, однако не обладает достаточной эффективностью. Однако стоит понимать, что при грамотном использовании своих данных и при соблюдении некоторых мер, риск утечки сведений может быть сведён к минимуму. Во многом уровень информационной безопасности зависит от уровня собственной компетенции человека в сфере использования информационно-коммуникационных технологий.

Литература

1. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных» // Справочно-правовая система «КонсультантПлюс».
2. Конвенция Совета Европы № 108 от 28 января 1981 года «О защите индивидуумов (частных лиц) при автоматизированной обработке персональных данных» // Справочно-правовая система «КонсультантПлюс».
3. Родичев Ю.А. Правовая защита персональных данных. Самара: Самарский университет, 2015. С. 39.
4. Хашева И.А. Практика использования информационно-коммуникационных технологий при оказании государственных услуг // Государственное и муниципальное управление. Ученые записки СКАГС. 2009.№4. С. 99-108.
5. Попов В.Г., Галиаскаров Д.Ф., Гвоздев Л.Б. Актуальность обеспечения информационной безопасности в сетях // StudNet. 2021. №4.
6. Мамаева Л.Н., Бехер В.В. Угрозы кибербезопасности в цифровом пространстве // Вестник Саратовского государственного социально-экономического университета. 2019. №4 (78).

Literature

1. Federal law of 27.07.2006 № 152-FZ (red. ot 21.07.2014) "On personal data" // legal reference system "ConsultantPlus".
2. The Council of Europe Convention No. 108 of 28 January 1981, "On the protection of individuals (individuals) with regard to automatic processing of personal data" // legal reference system "ConsultantPlus".
3. Rodichev Yu. a. Legal protection of personal data. Samara: Samara University, 2015. p. 39.
4. Khasheva I. A. Praktika ispolzovaniya informatsionno-kommunikatsionnykh tekhnologii pri obespechenii gosudarstvennykh uslug [The practice of using information and communication technologies in the provision of public services]. Uchenye Zapiski SKAGS. 2009.№4. P. 99-108.
5. Popov V. G., Galiaskarov D. F., L. B. Gvozdev the Relevance of information security in networks // StudNet. 2021. No. 4.
6. Mamaev, L. N., Becher V. cyber security Threats in the digital space // Bulletin of the Saratov state socio-economic University. 2019. №4 (78).