УДК 004.89

Лаврентьев С.А.
Lavrentyev S.A.
студент магистратуры
graduate student
2 курс, факультет ИБ
2 course Faculty IB
МФ МГТУ им. Н. Э. Баумана
MF MSTU them. N.E. Bauman
Россия, г. Москва
Russia, Moscow
Научный руководитель: Коннова Н.С.
scientific advisor Konnova N.S.
доцент, кандидат технических наук
Associate Professor, Candidate of Engineering Sciences

ПРАВОВОЕ РЕГУЛИРОВАНИЕ РАБОТЫ СИСТЕМЫ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ПО ГЕОМЕТРИИ ЛИЦА НА ОСНОВЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ

LEGAL REGULATION OF THE BIOMETRIC IDENTIFICATION SYSTEM BASED ON FACE GEOMETRY BASED ON MACHINE LEARNING ALGORITHMS

***Аннотация**: Биометрия человека входит в категорию персональных данных, следовательно система идентификации по биометрии должна быть достаточно безопасной для хранения и обработки подобных данных. В статье представлены законы, регламентирующие функционирование такой системы, а также приведен вывод о соответствии работы системы этим нормам и ограничениям.*

***Annotation**: Human biometrics is included in the category of personal data, so the biometrics identification system must be secure enough to store and process such data. The article presents the laws regulating the functioning of such a system, and also provides a conclusion about the compliance of the system with these norms and restrictions.*

***Ключевые слова**: нейронная сеть, биометрия, идентификация по геметрии лица.*

***Key words**: neural network, biometrics, the identity using face geometry*.

В современном мире технологии оказывают огромное влияние на повседневную жизнь каждого человека. Они делают ее удобней, комфортней и легче. Уже не является чем то новым оплачивать покупки бесконтактным способом с помощью телефона, или заказать практически любой товар через сеть Интернет и оплатить его.

Более того, в метро вводится бесконтактный пропуск, а в Америке запускаются магазины без наличия на выходе терминалов оплаты за покупки. Все это достигается за счет использовании систем биометрической идентификации.

При разработке системы распознавания образов на изображениях важно учитывать сферы информационных технологий и обеспечения безопасности информации. Для это в разделе приведены анализ и исследование нормативно-правовых документов Российской Федерации, которые регулируют использование биометрических и персональных данных. Такими документами являются:

- национальные стандарты в области биометрии и идентификации;
- конституция Российской Федерации;
- Федеральный закон “О персональных данных” от 27.07.2006 № 152-ФЗ;

- Федеральный закон “Об информации, информационных технологиях и о защите информации” от 27.07.2006 № 149-ФЗ;
- Федеральный закон “О техническом регулировании” от 27.12.2002 № 184-ФЗ;
- Постановление правительства Российской Федерации “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных” от 01.11.12 № 1119
- Постановление Правительства Российской Федерации “Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных” от 6.07.2008 № 512
- приказ ФСТЭК России “Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при обработке информационных системах персональных данных” от 18.02.2013 № 21;
- доктрина информационной безопасности Российской Федерации от 05.12.2016;
- гражданский кодекс РФ, часть первая №230-ФЗ от 18.12.2006 редакция 23.05.2018.

Конституция [1] – главный законодательный документ Российской Федерации, которая действует с 25.12.1995, применяется на всей территории страны и имеет наивысший приоритет среди других законов страны. В ней заключены правовые области, которые могут воздействовать на все сферы жизни гражданина РФ. Таким образом, создаваемый в работе комплекс должен иметь механизмы обработке и хранения информации

пользователей, также их безопасной передачи на сервер, не нарушая при этом описанные в разделе статьи Конституции.

ФЗ №149-ФЗ [2] используется вместо законов №254-ФЗ и №85-ФЗ и определяет положения при различных действиях с информацией таких, как поиск, создание и т.д. с использованием информационных систем и технологий и положений по защите информации.

Основополагающие принципы по информационной безопасности и технологий рассмотрены в статье 3. Указанным в ней ограничениям создаваемая система также должна соответствовать.

ФЗ №152-ФЗ РФ [3] необходим, чтобы обеспечить конфиденциальность персональных данных. Для этого был создан запрет на передачу, обработку и раскрытие данных третьим лицам без предварительного согласия владельца этих данных, а также если их владелец не нарушил законодательство РФ.

При этом персональные данные могут быть переданы третьим лицам если они используются, как статистические данные с исследовательской целью, но при этом предварительно такие данные необходимо обезличить [3]. Так же при обработке персональных данных следует учитывать уровень их обезличивания, поскольку при недостаточном обезличивании даже такую информацию можно отнести к категориям персональных данных.

Приказ №996 [4] необходим, для создания перечня мер, направленных для обезличивания персональных данных органами, являющихся государственными или муниципальными органами. Однако данные требования можно использовать как основополагающий или ориентированный документ для создания своих требований частными операторами. Также в документе нет разъяснений, к какой категории данный относятся обезличенные или являются отдельной категорией данных.

ФЗ “О техническом регулировании” от 27.12.2002 № 184-ФЗ [5] регулирует действия для сертификации продукции и установки соответствия с необходимыми требованиями, стандартами и условиями.

Эти требования носят обязательный характер, при котором принимаются решения об обязательной сертификации и реализуются согласно техническому регламенту или носят рекомендательный характер после подписании договора и, в некоторых случаях, после предоставлении сертификации.

В приказе ФСТЭК России “Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при обработке информационных системах персональных данных” от 18.02.2013 № 21 [6] описаны организационные и технические меры по обеспечению безопасности персональных данных. Они могут отличаться в зависимости от уровня защищенности персональных данных. Ими могут быть: аутентификация и идентификация субъектов и объектов доступа информационной системы, управление доступом, ограничение программной среды и т.д.

Помимо приказа № 21 [6] ФСТЭК определил угроз безопасности персональных данных при их обработке в информационной системе другими документами:

- ФСТЭК России 14.02.2008 [7] “Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных”;
- ФСТЭК России 15.02.2008 [8] “Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных”.

Доктрина информационной безопасности РФ [9] описывает задачи, которые необходимо решить, чтобы обеспечить информационную безопасность Российской Федерации. Также в данном документе отражены

национальные интересы по защите прав граждан, по использованию и обеспечения безопасности информации, сохранение работоспособности критических важных структур, развитие сфер областей информационной безопасности на международном уровне.

ГК РФ [10] содержит правила и рекомендации по охране интеллектуальной деятельности. При этом для работы создаваемых систем существует ряд ограничений. Исходя из них, создаваемый код приложения также является авторским и должен использоваться при согласии обладателя авторских прав.

Согласно постановлению Правительства РФ от 26.06.1995 № 608 "О сертификации средств защиты информации" [44] устанавливается порядок проведения сертификации средств защиты информации.

Процесс сертификации осуществляется участниками процесса сертификации, проводящих сертификацию по определённым установленным правилам, которые создаются федеральными органами по сертификации [11]:

- Федеральной службой по техническому и экспортному контролю;
- Федеральной службой безопасности Российской Федерации;
- Министерством обороны Российской Федерации.

Федеральные органы по сертификации, кроме того, что они создают систему сертификации и определяют правила аккредитации, выдают сертификаты и лицензии, рассматривают жалобы по сертификации, приостанавливают или отменяют работу выданного сертификата.

Согласно пункту 1 статьи 274 УК РФ [12] при нарушении правил эксплуатации оборудования информационно-телекоммуникационных сетей и правил доступа к ним, а так же нарушение правил при обработки и передачи охраняемой информации, которое привело к уничтожению, блокированию, модификации или копированию компьютерной информации, причинившее крупный ущерб, наказывается штрафом до 500

рублей или в размере заработной платы от иного дохода за период до 18 месяцев или исправительными работами до двух лет или наказывается исправительными работами до одного года или ограничение или лишение свободы до дух лет.

Согласно 2 пункту статьи 274 УК РФ [12] если действия привлекли тяжкие последствия то наказывается принудительными работами до 5 лет или лишение свободы до 5 лет.

Выводы

В современном мире информационные технологии затрагивают разные сферы жизни, что делает задачи по обеспечению безопасности многогранными и уделить особое внимание при разработке новых технологий.

При написании данной выпускной квалификационной работы были рассмотрены основные НПА и правовые акты, обеспечивающие и регулирующие информационную безопасность. Поскольку данная область имеет большое количество нормативно-правовых актов, то были рассмотрены основные из них.

При этом в разделе был выполнен обзор и анализ нормативного регулирования в сфере информационного безопасности и биометрических персональных данных, а также рассмотрены требования и стандарты для создаваемых систем, производящих обработку персональных данных.

Более того, в случае несоответствия работы действующему законодательству ответственность будет нести не только злоумышленник, но и ответственное лицо, не выполнившее требования.

Использованные источники

1. Консультант Плюс" - законодательство РФ: кодексы, законы, указы, постановления Правительства Российской Федерации, нормативные акты // Конституция Российской Федерации [Электронный документ].

URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (Дата обращения 23.02.2020).

2. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ [Электронный документ].
   URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (Дата обращения 23.02.2020).
3. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ [Электронный документ].
   URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (Дата обращения 23.02.2020).
4. Приказ Роскомнадзор "Об утверждении требований и методов по обезличиванию персональных данных" №996 от 05.09.2013 [Электронный документ]. URL: https://rg.ru/2013/09/18/dannye-dok.html (Дата обращения 23.02.2020).
5. Федеральный закон “О техническом регулировании” от 27.12.2002 № 184-ФЗ [Электронный документ].
   URL: http://www.consultant.ru/document/cons_doc_LAW_40241/ (Дата обращения 23.02.2020).
6. Приказ ФСТЭК России “Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при обработке информационных системах персональных данных” от 18.02.2013 № 21 [Электронный документ].
   URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (Дата обращения 23.02.2020).
7. ФСТЭК России 14.02.2008 [Электронный документ].
   URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-

dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god (Дата обращения 23.02.2020).

8. Приказ ФСТЭК России 15.02.2008 “Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных” [Электронный документ]. URL: https://fstec.ru/component/attachments/download/289 (Дата обращения 23.02.2020).
9. Доктрина информационной безопасности Российской Федерации от 05.12.2016 [Электронный документ]. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (Дата обращения 23.02.2020).
10. Гражданский кодекс РФ, часть первая №230-ФЗ от 18.12.2006 редакция 23.05.2018 [Электронный документ]. URL: http://www.consultant.ru/document/cons_doc_LAW_64629/ (Дата обращения 23.02.2020).
11. Постановление Правительства РФ от 26.06.1995 N 608 "О сертификации средств защиты информации" [Электронный документ]. URL: http://www.consultant.ru/document/cons_doc_LAW_7054/ (Дата обращения 23.02.2020).
12. УК РФ Статья 274 “Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей” от 07.12.2011 № 420-ФЗ [Электронный документ]. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9 (Дата обращения 23.02.2020).