КОМПЬЮТЕРНОЕ ОБЕСПЕЧЕНИЕ И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

DOI: 10.24143/2072-9502-2018-1-27-36
УДК [004.7.056:57.087.1]:347.02(470)

А. В. Антошечкин

АНАЛИЗ ВОЗМОЖНОСТЕЙ ПРИМЕНЕНИЯ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ ДЛЯ РЕАЛИЗАЦИИ ПРОЦЕДУР ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рассматривается задача использования биометрических методов для обезличивания персональных данных. Проведен анализ существующей российской и международной законодательно-нормативной базы по обезличиванию, выявлены несоответствия в определении этого понятия. В частности, выявлено, что обезличивание персональных данных в настоящее время не рассматривается как мера их защиты; обезличенные персональные данные не рассматриваются как категория персональных данных; обезличивание рассматривается как мера защиты, которая не отнесена непосредственно к мерам по обеспечению безопасности персональных данных, но, тем не менее, не позволит нарушить свойства их безопасности. Проведен анализ требований и методов по обезличиванию персональных данных. Выделены пять необходимых свойств обезличенных данных, четыре базовых метода обезличивания (введение идентификаторов, изменение состава и семантики, декомпозиция, перемешивание), а также три основные характеристики для методов обезличивания, связанные с обеспечением безопасности персональных данных. Анализ позволил выявить наличие или отсутствие перечисленных свойств и характеристик у каждого из рассмотренных методов обезличивания персональных данных. Рассмотрена задача хранения персональных данных и предложена процедура двухфакторной аутентификации на основе биометрических процедур при работе с базами персональных данных. Предложен метод обезличивания персональных данных на основе биометрических процедур, не предполагающий передачи конфиденциальной информации по каналам связи с использованием криптографии. Приведен пример реализации механизма обратимого обезличивания с использованием биометрических технологий.

Ключевые слова: персональные данные, обезличивание, методы обезличивания, биометрические данные, двухфакторная аутентификация.

Введение

27 июля 2017 года Федеральному закону РФ № 152-ФЗ «О персональных данных» исполнилось одиннадцать лет [1]. В стране принимаются определённые меры по реализации этого закона. Нормативная и методическая базы совершенствуются, однако до идеальной реализации положений закона ещё далеко. Это объясняется тем, что до принятия соответствующих законодательных актов, связанных с защитой информации, в том числе и персональных данных, международная сеть информационного обмена уже существовала, и в ней, к моменту принятия указанных законодательных актов, оказалось аккумулированным большое количество информации, критичной с точки зрения неприкосновенности частной жизни человека и гражданина. И даже при самых благоприятных прогнозах при неукоснительном выполнении положений Закона № 152-ФЗ информация частного характера, накопленная в Интернете, будет влиять на общее впечатление об эффективности российского законодательства в области обеспечения безопасности персональных данных.

Целью Закона «О персональных данных» является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. В частности, на операторов

и иных лиц, получивших доступ к персональным данным, возлагается обязанность по обеспечению их конфиденциальности – «…не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом» [1, ст. 7]. Ранее делалось исключение для случая обезличивания персональных данных, а также в отношении общедоступных персональных данных. Настоящая редакция Федерального закона является более строгой с точки зрения обеспечения конфиденциальности персональных данных с учетом более расширенного понимания определения понятия «персональные данные».

Обезличивание персональных данных

Федеральным законом вводится понятие «обезличивание персональных данных» – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных [1, п. 9 ст. 3], что подразумевает обратимость процедуры обезличивания. В предыдущей редакции Федерального закона при ссылке на обезличивание персональных данных речь шла о действиях, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных, т. е. процедура обезличивания рассматривалась как необратимая. Такой же подход существовал и при определении категорий персональных данных, обрабатываемых в информационных системах персональных данных (ИСПДн), и классификации ИСПДн в соответствии с ранее действовавшим совместным приказом от 13 февраля 2008 г. Федеральной службы по техническому и экспортному контролю (ФСТЭК) России № 55, ФСБ России № 86, Министерства информационных технологий и связи Российской Федерации № 20 «Об утверждении порядка проведения классификации информационных систем персональных данных» (https://rg.ru/2008/04/12/informaciya-doc.html), в котором обезличенные данные и общедоступные данные приравнивались к одной – четвертой категории персональных данных с минимальными требованиями по их защите.

В п. 2 ст. 19 Федерального закона перечисляются возможные меры по обеспечению безопасности персональных данных. Непосредственно к таковым мерам обезличивание персональных данных не отнесено. Применение процедуры обезличивания, в соответствии с Федеральным законом, предусматривается как обязательная процедура при осуществлении обработки персональных данных в статистических или иных исследовательских целях [1, пп. 9 п. 1 ст. 6].

Для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, в соответствии с ч. 3 ст. 18.1 Федерального закона «О персональных данных» постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 утверждён перечень соответствующих мер. В первоначальной редакции документа, наряду с другими документами, связанными с обработкой персональных данных, требовалось наличие разработанных документов, связанных с обезличиванием персональных данных. Это позволяло сделать вывод о необходимости проведения таких мероприятий при обработке персональных данных.

В новую редакцию документа постановлением Правительства Российской Федерации от 6 сентября 2014 г. № 911 внесены изменения, говорящие о необходимости наличия документов по обезличиванию только при условии обезличивания персональных данных.

При создании системы защиты в ИСПДн, в том числе государственных ИСПДн, оператором принимаются организационные и технические меры по нейтрализации актуальных угроз безопасности информации.

В любом случае для информационной системы применение обезличивания персональных данных в качестве защитной меры для достижения целей, определённых Федеральным законом, не может послужить поводом для снижения требуемого уровня защищенности персональных данных в целом для информационной системы. Дело в том, что для обеспечения отдельных свойств обезличенных персональных данных требуется сохранение некоторой ключевой информации, которую необходимо защищать на том же уровне, что и необезличенную информацию, содержащую персональные данные. Снижение требуемого уровня защищенности персональных данных может быть применено только для отдельных сегментов информационной системы, в которой хранятся обезличенные данные без ключевой информации, позволяющей провести процедуру, обратную обезличиванию. В целом для целей ИСПДн требуемый уровень за-

щищенности персональных данных не изменится. Это подтверждается тем, что в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных» (http://www.consultant.ru/document/cons_doc_LAW_137356/), утвержденными Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 (далее – Требования к защите персональных данных), необходимость обеспечения того или иного уровня защищенности персональных данных при их обработке в информационной системе не связывается с обезличиванием персональных данных в данной системе. Такая категория персональных данных в Требованиях к защите персональных данных отсутствует, а к категории иных персональных данных обезличенные персональные данные отнести нельзя без некоторых уточнений, касающихся категории и требований по защите ключевой информации, позволяющей провести процедуру, обратную обезличиванию. Аналогично в «Составе и содержании организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных приказом ФСТЭК России от 18 февраля 2013 года № 21 (https://fstec.ru/component/attachments/download/562), не упоминается возможность использования обезличивания персональных данных для реализации какой-либо из мер по обеспечению безопасности персональных данных.

Таким образом, анализ Федерального закона и принятых в соответствии с ним нормативных правовых актов показывает, что обезличивание персональных данных в настоящее время не рассматривается как мера их защиты, а обезличенные персональные данные не рассматриваются как категория персональных данных для определения требуемого уровня защищенности этих данных при их обработке в ИСПДн. Сам процесс обезличивания в понятиях Федерального закона является обработкой персональных данных, т. е. действием (операцией) или совокупностью действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными [1, п. 3 ст. 3].

Требования и методы по обезличиванию персональных данных

Вопрос обезличивания персональных данных при создании системы защиты информации операторами обычно не рассматривается, между тем обработка персональных данных в статистических или иных исследовательских целях при этом может проводиться с использованием персональных данных, содержащихся в ИСПДн. В данном случае проведение обезличивания и может стать той мерой защиты, которая не отнесена непосредственно к мерам по обеспечению безопасности персональных данных, но не позволит нарушить свойства безопасности персональных данных при достижении указанных статистических или иных исследовательских целей. Такая возможность подтверждается и тем, что в соответствии с пп. «з» п. 1 «Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» (http://base.garant.ru/70152982/), разработаны и утверждены приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 «Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ» (Далее – Требования и методы обезличивания (http://www.consultant.ru/document/cons_doc_LAW_151882/)). Этим приказом обезличивание персональных данных фактически признаётся мерой защиты персональных данных и должно обеспечивать не только их защиту от несанкционированного использования, но и возможность их обработки. Для этого обезличенные данные должны обладать свойствами, сохраняющими основные характеристики обезличиваемых персональных данных (п. 3 Требований и методов обезличивания). Действие данного документа распространяется на операторов, являющихся государственными или муниципальными органами. Для других операторов информационных систем данный документ может носить рекомендательный характер.

Между тем Требованиями и методами обезличивания устанавливаются:

– свойства обезличенных данных (полнота, структурированность, релевантность, семантическая целостность, применимость, анонимность);

– характеристики методов обезличивания персональных данных (обратимость, вариативность, стойкость, возможность косвенного деобезличивания, совместимость, параметрический объем, возможность оценки качества данных);

– требования к свойствам получаемых обезличенных данных (сохранение полноты, сохранение структурированности обезличиваемых персональных данных, сохранение семантической целостности обезличиваемых персональных данных, анонимность отдельных данных не ниже заданного уровня);

– требования к свойствам метода обезличивания (обратимость, возможность обеспечения заданного уровня анонимности, увеличение стойкости при увеличении объема обезличиваемых персональных данных).

По набору тех или иных свойств и характеристик в документе определены наиболее перспективные и удобные для практического применения методы обезличивания:

– метод введения идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);

– метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);

– метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);

– метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

Соответствие методов обезличивания персональных данных свойствам обезличенных данных [2], а также характеристики методов обезличивания приведены в табл. 1, 2.

Таблица 1

Свойства обезличенных персональных данных*

Метод обезличивания / Свойства обезличенных данных	Метод введения идентификаторов	Метод изменения состава и семантики	Метод декомпозиции	Метод перемешивания
Полнота	+	+/–	+	+
Структурированность	+	+	+	+
Релевантность	+/-	+	+	+
Семантическая целостность	+	+/–	+	+
Применимость	+	+	+	+
Анонимность	+/–	+	+/–	+

* Знак «+» – безусловное наличие свойства или характеристики метода; знаки «+/–» – условное наличие свойства или характеристики метода; знак «–» – отсутствие свойства (характеристики) независимо от дополнительно принимаемых мер.

Таблица 2

Методы обезличивания персональных данных*

Метод обезличивания / Характеристики методов	Метод введения идентификаторов	Метод изменения состава и семантики	Метод декомпозиции	Метод перемешивания
Обратимость метода	+	–	+	+
Невозможность косвенного деобезличивания	+	+	-	+
Стойкость	+/–	+	+/–	+/–

* Знак «+» – безусловное наличие свойства или характеристики метода; знаки «+/–» – условное наличие свойства или характеристики метода; знак «–» – отсутствие свойства (характеристики) независимо от дополнительно принимаемых мер.

Анализ предлагаемых методов позволяет понять, что для достижения целей, указанных в Федеральном законе, для которых применяется обезличивание персональных данных, необходима анонимность, и это прямо указано в определении, данном в Федеральном законе, и в Требованиях и методах обезличивания. Однако этим свойством по умолчанию не обладают два из указанных четырех методов. При реализации обезличивания персональных данных методом введения идентификаторов или методом декомпозиции оператор должен обеспечивать выпол-

нение дополнительных условий. Кроме того, метод изменения состава или семантики не обеспечивает обратимость процедуры обезличивания. Такое разделение методов обезличивания с точки зрения возможностей обеспечения анонимности и обратимости обезличивания объясняется тем, что Федеральным законом в настоящее время под обезличиванием понимается обратимая процедура, обеспечивающая анонимность субъекта персональных данных, а Требования и методы обезличивания разработаны с точки зрения более широкого понимания обезличенной информации, в том числе с использованием мирового опыта работы с обезличенными и анонимными данными. В частности, документом NIST SP 800-122 «Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)» [3] предусматриваются два понятия: «обезличенная информация» (De-Identifying Information) и «анонимная информация» (Anonymizing Information). С учетом того, что в понятиях Федерального закона анонимная информация не считается персональными данными и в законе не указано о необходимости её защиты с точки зрения защиты персональных данных, применение Требований и методов обезличивания должно быть ограничено с точки зрения их применимости к обезличиванию персональных данных для достижения целей, определённых в соответствии с Федеральным законом. Кроме того, процесс получения из персональных данных анонимной информации требует отдельного регулирования и, возможно, может быть реализован, в том числе с использованием Требований и методов обезличивания.

На практике обезличивание может встречаться достаточно часто, например, в виде некоторого «технологического» обезличивания при введении ключевых полей в реляционных базах данных, которые, в свою очередь, обрабатываются в единой СУБД, в которой представлена вся информация, содержащая персональные данные. Формально для её получения в удобочитаемом виде необходимо использовать дополнительную информацию (выполнить запрос, сформировать отчет или вывод данных с расшифровкой в окне формы и т. д.), что указано в определении процедуры обезличивания персональных данных. Законодательно порядок проведения таких мероприятий не урегулирован, они не имеют в данной ситуации цели защиты информации, их реализация обусловлена лишь принципами функционирования СУБД.

Вывод о реализуемости перечисленных выше методов обезличивания персональных данных возможно сделать по итогам их реализации в отдельных программных продуктах или с использованием различных информационных технологий.

Применимость биометрических данных для двухфакторной аутентификации

Одним из принципов обработки персональных данных является требование о хранении персональных данных в форме, позволяющей определить субъекта персональных данных, в течение времени не большего, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных дополнительно не установлен. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом [1, п. 7 ст. 5]. Такой подход может создавать определённые сложности, когда обработка персональных данных проводится эпизодически, с большими перерывами во времени, но при очередном случае обработки персональных данных было бы неудобно вводить их вновь в ИСПДн и потребовало бы для этого дополнительного времени. В таком случае хранение персональных данных во временных промежутках между непосредственной обработкой персональных данных должно осуществляться либо по дополнительному соглашению, либо в обезличенном виде с возможностью проведения процедуры обратной обезличиванию.

Одним из методов такого «обратимого» обезличивания, который реализуется сравнительно просто, мог бы стать метод введения идентификаторов. Введение идентификаторов для каждой записи в базе данных и замена персональных данных таким идентификатором аналогична созданию пары значений: «идентификатор» и «аутентификационная информация». При этом в соответствующем поле каждой записи в базе данных остается храниться идентификатор, а персональные данные хранятся либо в зашифрованном виде в обезличенной базе данных, либо в открытом виде в отдельном месте хранения. С точки зрения формы представления аутентификационной информации для обратного преобразования обезличенных персональных данных в идентифицируемую информацию возможно использование для каждой записи в базе данных

своего пароля, как давно проверенного средства, известного только субъекту персональных данных. Однако, по статистике исследований [4], более 80 % инцидентов в области информационной безопасности были связаны с применением недостаточно стойких паролей. Применение паролей различной сложности порождает противоречие: с одной стороны применение слабых паролей означает слабую защиту информации, применение сложных паролей порождает проблему их запоминания и фиксацию данной информации на каком-либо доступном носителе в доступном месте. Это противоречие может устранить внедрение двухфакторной аутентификации, использующей для аутентификации несколько факторов, в том числе с использованием одноразовых паролей в SMS-сообщении на мобильный телефон или одноразовых паролей, доставляемых по адресу электронной почты. Это существенно повышает безопасность использования информации, но не спасает, например, при взломе электронной почты с использованием знания ответа на «секретный вопрос». Далее возможно поменять «забытый пароль» к любому из известных злоумышленнику сервисов, привязанных к данному адресу электронной почты: аккаунты социальных сетей, доступ к сервисам сайта государственных услуг, личный кабинет налогоплательщика, облачное хранилище данных и т. д.

Количество вариантов представления аутентификационной информации в системах с двухфакторной аутентификацией достаточно большое, и с учетом непрерывного развития информационных технологий их количество растёт. Примером могут служить различные программно-аппаратные решения, такие как автономные ключи для генерации одноразовых паролей, считыватели RFID-меток, криптокалькуляторы, программные и аппаратные жетоны (токены), электронные ключи различных типов – Touch Memory и ключ/смарт-карта. Все эти и другие существующие средства многофакторной аутентификации могут быть интегрированы между собой, работать поочередно и в комплексе [4, 5].

Ключевой информацией в методах обратимого обезличивания для восстановления обезличенной информации может стать использование биометрических решений для обезличивания персональных данных и, при необходимости, – для обратного преобразования. Биометрия – это технология идентификации объекта (личности человека) на основе измерений его индивидуальных характеристик. Основные достоинства такого решения для обратимого обезличивания заключаются в том, что биометрические характеристики трудно потерять, подделать или передать другому человеку, использование этой технологии – фактическое выполнение ст. 9 Федерального закона 152-ФЗ, связанной с согласием субъекта персональных данных на их обработку. Недостатками биометрических решений, в свою очередь, являются: нетривиальность ввода биометрической информации, невозможность изменения пользователем биометрического «пароля» к системе.

В литературе [6] приводятся примеры биометрических характеристик и алгоритмов, использующихся при обработке биометрических данных. К таковым относятся:

– радужная оболочка глаза, которая является устойчивой характеристикой и в настоящее время считается самой надёжной идентификационной характеристикой личности;

– отпечаток пальца, для которого основой методов анализа является выделение на изображении особых точек: ветвления и конца папиллярных линий (отпечаток пальца является более слабым признаком по сравнению с радужной оболочкой глаза);

– ладонь – используются несколько биометрических характеристик (циркулярное разложение бинарного изображения, представление изображения в виде гибкого объекта, граничноскелетное представление, трехмерное сканирование ладони);

– лицо – с точки зрения использования в системах распознавания предоставляет преимущества реализации без дорогостоящего оборудования и бесконтактного способа регистрации;

– динамическая аутентификация, как метод распознавания, может использовать в качестве характеристики динамическую подпись или голос человека.

Наиболее перспективными считаются мультимодальные биометрические системы, использующие разнородные биометрические характеристики человека и создающие более информативные шаблоны. Наиболее точным в настоящее время считается распознавание по радужной оболочке глаза и по отпечатку пальца.

Создание дополнительного объекта защиты при совершенствовании подсистемы защиты информации в виде дополнительной базы биометрических данных нецелесообразно и во многих

случаях связано с дополнительными рисками. Между тем, согласно Требованиям к защите персональных данных, параметры необходимости обеспечения того или иного уровня защищенности биометрических персональных данных соответствуют параметрам обеспечения такого же уровня защищенности для специальных категорий персональных данных для количества менее 100 000 записей о субъектах персональных данных. Для количества более 100 000 записей требуемый уровень защищенности специальных категорий персональных данных не ниже требуемого уровня защищенности соответствующих биометрических данных. Это позволяет, не увеличивая требуемый уровень защищенности персональных данных, осуществлять их хранение в ИСПДн, обрабатывающей специальные категории персональных данных, соответствующие биометрические персональные данные.

Использование биометрических характеристик в информационных системах предполагает хранение в них и биометрических шаблонов-эталонов. При широком внедрении средств биометрии базы данных с биометрической информацией могут подвергаться краже и дальнейшему анализу злоумышленниками. Поскольку биометрические данные, идентифицирующие субъекта персональных данных, остаются практически неизменными в течение жизни, сменить биометрический «пароль» крайне сложно, а во многих случаях – просто невозможно. Выходом из данной ситуации может стать хранение биометрической информации в некотором закодированном виде, например в виде некоторой хэш-функции, по аналогии с хранением обычных паролей в защищенных системах. Однако, по данным различных исследований [6], прямое применение криптографического аппарата хэширования к биометрическим системам невозможно, поскольку невозможно обеспечить выполнение требований к хэш-функциям, которые должны обладать определенными свойствами. К таким свойствам относятся: односторонность, ничтожно малая вероятность совпадения хэш-функций двух разных входных массивов, наличие лавинного эффекта. Причина – «нечеткость» биометрических данных в том смысле, что они, при общей своей неизменности, могут несколько изменяться у одного и того же объекта с течением времени (порез пальца, изменение голоса, воспаление глазной оболочки и др.).

Типовое применение биометрических данных [7] – это их применение в качестве идентифицирующей и аутентифицирующей информации при входе в информационную систему со всеми имеющимися преимуществами и недостатками. Наиболее распространенными в настоящее время при работе с биометрическими данными стали три способа реализации: «всё в одном» (в одном приборе объединены все сущности: считыватель, верификатор, работа с эталоном); «эталон передаётся снаружи» (прибор считывает биометрический параметр и верифицирует его с переданным в него эталоном); «эталон в базе» (прибор считывает биометрический параметр и передаёт его в верификатор, функционирующий в операционной системе, для поиска соответствующего эталона в базе эталонов). Для дальнейшего рассмотрения оптимальной с точки зрения подсистемы информационной безопасности является вторая схема.

Для реализации такой схемы производители средств защиты информации предлагают варианты [8], когда биометрическая информация не хранится в защищаемой информационной системе, а находится у пользователя в виде некоторого идентификатора вместе с собственно его биометрическими данными (отпечатками пальцев, рисунком сосудистого русла, сетчаткой глаз и т. д.). Процесс аутентификации реализуется в виде предъявления идентификатора и биометрического признака – на идентификаторе хранится биометрический эталон, а биометрический признак получается от одного из соответствующих сканеров. По предъявленным данным проводится операция верификации, результат которой становится результатом аутентификации, идентификация проводится по предъявленному идентификатору. Такой вариант возможен в программно-аппаратных комплексах Аккорд-Win32 и Аккорд-Win64 [5].

Предлагаемая в данном случае аппаратная реализация – три типа считывателей:

– сканер сосудистого русла, совмещённый с манипулятором типа «мышь», дополненным подставкой для удобства размещения руки над сканером (PalmSecure);

– сканер сосудистого русла, совмещённый со считывателем контактной смарт-карты (PalmSecure);

– сканер отпечатка пальца, совмещённый со считывателем контактной смарт-карты (BioLink).

Метод обезличивания персональных данных с использованием биометрических технологий

С учетом указанной выше возможности хранения биометрических данных (эталонов) вне информационной системы можно предлагать различные варианты использования такого подхода, в том числе не только для идентификации и аутентификации при входе в систему. Может быть предложен вариант обратимого обезличивания специальных категорий персональных данных, реализуемого с использованием биометрических данных субъекта персональных данных, эталонные данные которых хранятся во внешнем устройстве, находящемся у субъекта персональных данных. Процедура деобезличивания проводится при непосредственном предъявлении субъектом персональных данных устройства с хранящейся на нём эталонной биометрической информацией и собственного биометрического признака для их сравнения и выполнения алгоритма деобезличивания данных в целях дальнейших действий с персональными данными специальных категорий персональных данных конкретного субъекта персональных данных. Такой механизм может быть предложен для недопущения несанкционированных лично субъектом персональных данных (незаконных) действий со специальными категориями его персональных данных, невозможностью обработки этих данных без непосредственного участия субъекта персональных данных. В частности, «Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [9] при классификации угроз безопасности персональных данных по видам возможных источников угроз безопасности персональных данных выделяется класс угроз, связанных с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн (внутренний нарушитель). Нарушитель такого типа может целенаправленно или случайно нанести вред как субъекту персональных данных, так и самому оператору персональных данных. Несанкционированные действия внутреннего нарушителя возможно существенно ограничить с использованием предложенного выше метода обратимого обезличивания. В упрощенном случае эталонные данные возможно хранить не во внешнем устройстве, находящемся у субъекта персональных данных, а на сервере, хранящем и обрабатывающем специальные категории персональных данных, реализуемые мероприятия по защите которых соответствуют требованиям по защите соответствующих биометрических данных.

Порядок построения систем аутентификации, использующих биометрическую информацию, с заявленными вероятностями ошибочного пропуска «Чужого» менее 10^{-12} регламентируется национальным стандартом Российской Федерации ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадёжной биометрической аутентификации» (http://docs.cntd.ru/document/1200048922) и другими национальными стандартами из этой серии. При этом предполагается использование процедур обработки биометрической информации и преобразователей нечетких (неоднозначных) биометрических образов пользователя в его длинный пароль или ключ, используемый далее в одной из процедур высоконадежной криптографической аутентификации. В национальных стандартах для систем высоконадежной биометрической аутентификации требования достаточно строги с точки зрения необходимости гарантированного уничтожения конфиденциальной информации с биометрическим образом пользователя и кода ключа пользователя, а также необходимости выполнения организационно-технических мероприятий, исключающих перехват указанной выше конфиденциальной информации через каналы визуального наблюдения, акустического прослушивания, побочных электромагнитных излучений и наводок при проведении процедуры тестирования и обучения нейросетевой защиты [10].

Заключение

Предлагаемый метод обезличивания персональных данных не предполагает передачи конфиденциальной информации по каналам связи с использованием криптографии, поэтому для его реализации с использованием биометрических технологий допустимо использовать требования к средствам биометрической аутентификации с вероятностью ошибочного пропуска «Чужого» большей, чем указано выше, регламентированные системой международных стандартов, разработанных ISO/IEC JTC1 SC37 и гармонизированных ТК 355 ПК 7 «Биометрическая идентификация» [10].

Примером реализации механизма обратимого обезличивания с использованием биометрических технологий может служить невозможность без непосредственного участия больного (субъекта персональных данных) оформления фиктивного посещения медицинского учреждения больным с оформлением предоставленного фиктивно объёма медицинских услуг, которые в дальнейшем оплачиваются фондом медицинского страхования. Невозможно будет также выписать льготный рецепт и получить льготные лекарства на имя некоторого лица из числа льготных категорий граждан без его непосредственного участия. В условиях скудного финансирования медицинского бюджета это сэкономит средства Фонда обязательного медицинского страхования, которых может не хватать для реального лечения больных.

СПИСОК ЛИТЕРАТУРЫ

1. *О персональных* данных: Федеральный закон от 27 июля 2006 года № 152-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_61801.

2. *Об утверждении* требований и методов по обезличиванию персональных данных // Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=157082&fld=134&dst=1000000001,0&rnd=0.3187907696471066#0 (дата обращения: 22.12.2017).

3. *National* Institute of Standards and Technology. Special Publication 800-122 Natl. Inst. Stand. Technol. Spec. Publ. 800-122, 59 p. (Apr. 2010). URL: https://lovedoc.org/embed/sp800-122.

4. *Авдосьев Д.* Проблема человеческого фактора в технологиях аутентификации. Недостатки и методы решения // Защита информации. Инсайд. 2012. № 5 (47). С. 69–71.

5. *Наместников Г. А., Крылова М. И.* Российские системы двухфакторной аутентификации: просто, удобно, без проблем // Защита информации. Инсайд. 2017. № 5 (77). С. 42–45.

6. *Александров Я. А.* Биометрическая идентификация // Защита информации. Инсайд. 2012. № 3 (45). С. 82–88.

7. *Конявская С. В., Счастный Д. Ю., Лыдин С. С.* Биометрия и защита информации: человеческий признак против человеческого фактора // Защита информации. Инсайд. 2013. № 6 (54). С. 52–57.

8. *ЗАО «ОКБ САПР».* URL: http://www.accord.ru (дата обращения: 22.12.2017).

9. *Базовая модель* угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Федеральной службой по техническому и экспортному контролю 15 февраля 2008 г.). URL: http://docs.cntd.ru/document/902330983.

10. *ГОСТ ISO/IEC 19794-1-2015*. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Ч. 1. Структура. URL: http://docs.cntd.ru/document/1200129505.

Статья поступила в редакцию 22.11.2017

ИНФОРМАЦИЯ ОБ АВТОРЕ

Антошечкин Алексей Вячеславович – Россия, 414056, Астрахань; Астраханский государственный технический университет; доцент кафедры информационной безопасности; vkao1@mail.ru.

A. V. Antoshechkin

ANALYSIS OF POSSIBILITIES OF BIOMETRIC TECHNIQUES APPLICATION FOR CARRYING OUT DEPERSONALIZATION OF PERSONAL DATA

Abstract. The paper focuses on the problem of using biometric methods for the depersonalization of personal data. The analysis of the existing Russian and international legislative and regulatory framework for depersonalization has been carried out, and inconsistencies in the weakening of this concept have been revealed. In particular, it was found out that depersonalization of the personal data is not currently considered as a measure of their protection, personalized personal data

are not treated as a category of personal data, depersonalization is considered a protection measure that is not directly related to measures to ensure the security of personal data, but not will disrupt the properties of their security. The analysis of requirements and methods for the depersonalization of personal data was carried out. There have been identified 5 necessary properties of impersonal data; 4 basic methods of depersonalization (introduction of identifiers, changes in composition and semantics, decomposition, mixing), and 3 main characteristics for the methods of depersonalization related to the security of personal data. The analysis elicited the presence or absence of the listed characteristics in each method of depersonalization of personal data. The problem of storing personal data has been considered, and the procedure of using a two-factor authentication based on biometric methods for working with personal data bases has been proposed. A method of depersonalization of personal data based on biometric procedures not supposing supply of confidential information via communication channels using cryptography has been proposed. To demonstrate the efficiency of the method there was given an example of reversible depersonalization using biometric techniques.

Key words: personal data, depersonalization, methods of depersonalization, biometric data, two-factor authentication.

REFERENCES

1. *O personal'nykh dannykh: Federal'nyi zakon ot 27 iiulia 2006 goda № 152-FZ* [On the personal data: Federal Law No. 152-F3 dated July 27, 2006]. Available at: http://www.consultant.ru/document/cons_doc_LAW_61801.

2. *Ob utverzhdenii trebovanii i metodov po obezlichivaniiu personal'nykh dannykh* [On establishing requirements and methods of depersonalization of personal data]. Metodicheskie rekomendatsii po primeneniiu prikaza Roskomnadzora ot 5 sentiabria 2013 g. № 996. Available at: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=157082&fld=134&dst=1000000001,0&rnd=0.3187907696471066#0 (accessed: 22.12.2017).

3. *National Institute of Standards and Technology.* Special Publication 800-122 Natl. Inst. Stand. Technol. Spec. Publ. 800-122, 59 p. (Apr. 2010). Available at: https://lovedoc.org/embed/sp800-122.

4. Avdos'ev D. Problema chelovecheskogo faktora v tekhnologiiakh autentifikatsii. Nedostatki i metody resheniia [Problem the human element in authentication techniques. Weak points and methods of solution]. *Zashchita informatsii. Insaid*, 2012, no. 5 (47), pp. 69-71.

5. Namestnikov G. A., Krylova M. I. Rossiiskie sistemy dvukhfaktornoi autentifikatsii: prosto, udobno, bez problem [The Russian two-factor authentication systems: simple, convenient and flawless]. *Zashchita informatsii*. Insaid, 2017, no. 5 (77), pp. 42-45.

6. Aleksandrov Ia. A. Biometricheskaia identifikatsiia [Biometric identification]. *Zashchita informatsii. Insaid*, 2012, no. 3 (45), pp. 82-88.

7. Koniavskaia S. V., Schastnyi D. Iu., Lydin S. S. Biometriia i zashchita informatsii: chelovecheskii priznak protiv chelovecheskogo faktora [Biometry and information security: human indicator vs human element]. *Zashchita informatsii. Insaid*, 2013, no. 6(54), pp. 52-57.

8. *ZAO «OKB SAPR»* [CJSC "OKB SAPR"]. Available at: http://www.accord.ru (accessed: 22.12.2017).

9. *Bazovaia model' ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh* [The basic model of threats to the security of personal data during their processing in personal data information systems]. Utverzhdena Federal'noi sluzhboi po tekhnicheskomu i eksportnomu kontroliu 15 fevralia 2008 g.). Available at: http://docs.cntd.ru/document/902330983.

10. *GOST ISO/IEC 19794-1-2015. Informatsionnye tekhnologii. Biometriia. Formaty obmena biometricheskimi dannymi. Ch. 1. Struktura* [Information technology. Biometrics. Biometric data interchange formats. Part 1. Framework]. Available at: http://docs.cntd.ru/document/1200129505.

The article submitted to the editors 22.11.2017

INFORMATION ABOUT THE AUTHOR

Antoshechkin Alexey Vyacheslavovich – Russia, 414056, Astrakhan; Astrakhan State Technical University; Assistant Professor of the Department of the Information Security; vkao1@mail.ru.