

ОБРАБОТКА ИНФОРМАЦИИ. ПРОГРАММНЫЕ КОМПЛЕКСЫ

УДК 004.056

СПОСОБ ИДЕНТИФИКАЦИИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПО ОБЕЗЛИЧЕННЫМ ДАННЫМ

Е.С. Волокитина

*ФГБОУ ВПО «Юго-Западный государственный университет»,
г. Курск*

Рецензент д-р физ.-мат. наук, профессор В.П. Добрица

Ключевые слова и фразы: аутентификация; безопасность информации; идентификация; информационная система персональных данных; персональные данные; система идентификации; субъект персональных данных.

Аннотация: Разработан способ идентификации физического лица с использованием обезличенной базы данных, с целью выполнения требования Федерального закона «О персональных данных» и оптимизации затрат организации-оператора, обрабатывающей персональные данные.

С целью выполнения требований Федерального закона «О персональных данных» организация-оператор, обрабатывающая персональные данные (ПДн) физических лиц, может принять решение о том, чтобы произвести обезличивание персональных данных для хранения их в информационной системе персональных данных (ИСПДн). Это позволит снизить требования к хранению информационной системы, повысит надежность идентификации физического лица и обеспечит возможность аутентификации субъекта, предъявившего идентификатор системе. При обращении субъекта организация должна произвести его идентификацию в обезличенной базе данных (ОБД).

Рассмотрим модель системы идентификации физического лица с использованием обезличивания ПДн на примере организации, обрабатывающей персональные данные в ИСПДн с целью оказания услуг.

Волокитина Евгения Сергеевна – преподаватель кафедры «Комплексная защита информационных систем», e-mail: eva_kursk@mail.ru, ФГБОУ ВПО «Юго-Западный государственный университет», г. Курск.

В случае, если организация принимает решение не обезличивать данные, обработка ведется на всех ПЭВМ, где есть доступ к базе данных (БД) с персональными данными. При этом, согласно требований Федерального закона «О персональных данных» ст. 18.1 п. 1.3 [1], необходимо обеспечивать безопасность хранящихся персональных данных. Для снижения затрат организация-оператор может использовать предлагаемый в данной статье способ идентификации субъекта персональных данных по обезличенным данным.

Для обеспечения реализации предлагаемого способа требуется выполнение следующих условий:

- физическое лицо должно быть зарегистрировано в системе;
- при регистрации ему выдается внешний носитель, на котором содержится уникальный идентификационный ключ, который также находится в обезличенной базе данных ИСПДн1 и базе данных ИСПДн2;
- физическое лицо предоставляет организации-оператору номер телефона устройства санкционирования доступа с SIM-картой для последующего получения на него кода подтверждения доступа. В обезличенной базе данных ИСПДн1 вводим поле, содержащее сообщаемый субъектом номер.

С целью обезличивания персональных данных предлагается выполнить следующие действия.

1. Исходную базу данных переносим на локальную сеть, не подключенную к общей сети организации.

2. Вводим дополнительное поле, содержащее уникальный идентификационный ключ [2]. Данный уникальный идентификационный ключ, присутствующий в обеих БД, записываем на внешний носитель, который будет находиться у физического лица. Данную ОБД ИСПДн1 располагаем на ПЭВМ сети организации.

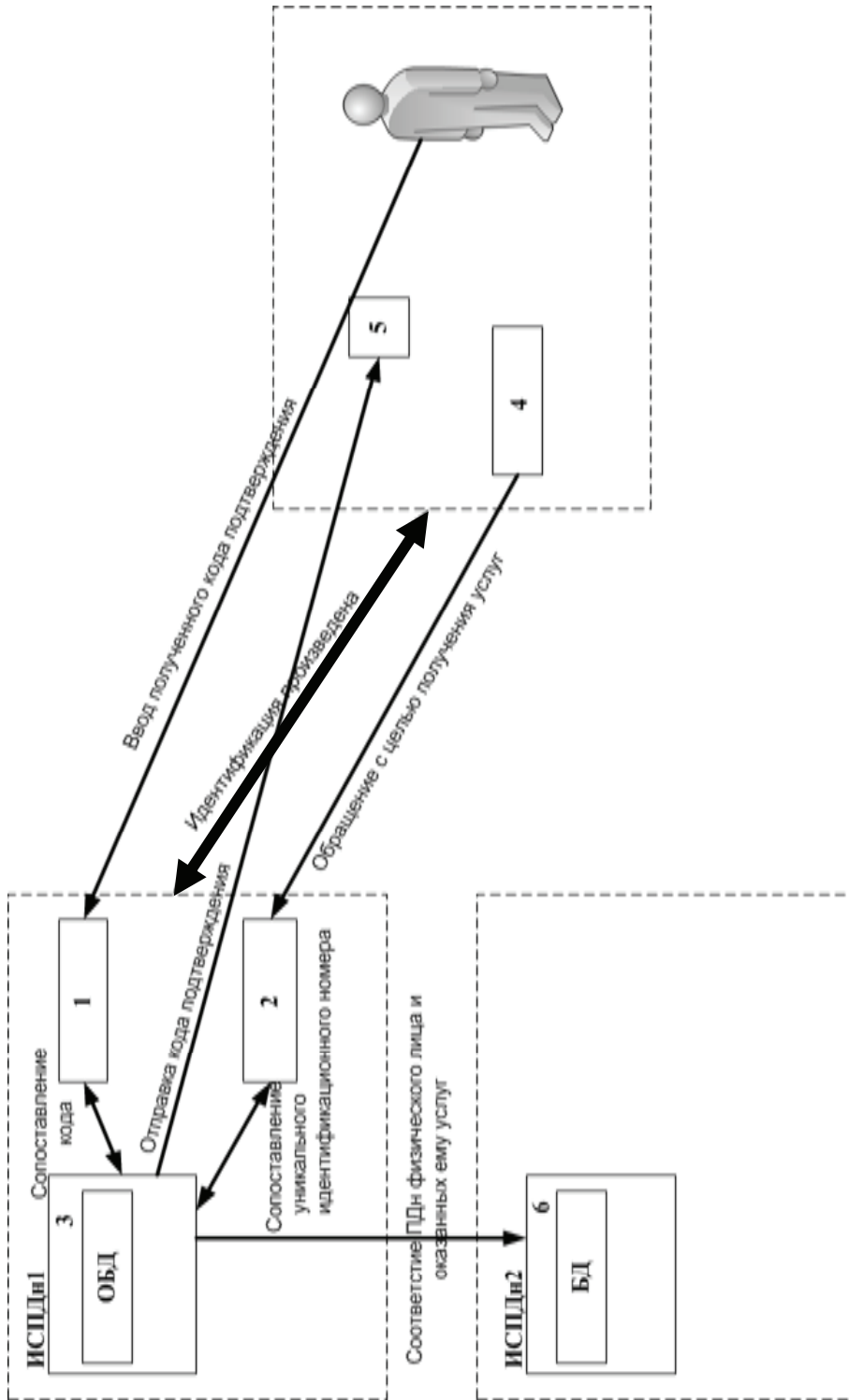
3. Создаем из исходной базы данных ОБД путем удаления всех однозначно идентифицирующих данных.

4. Дополняем полем индивидуального номера телефона устройства санкционирования доступа на базе устройства с SIM-картой физического лица.

Графическое представление способа идентификации субъекта персональных данных по обезличенным данным представлено на рисунке.

В способе описываются следующие блоки:

- 1 – блок ввода;
- 2 – блок регистрации, содержащий устройство считывания уникального персонального обезличенного идентификатора физического лица с внешнего носителя;
- 3 – блок обработки ИСПДн1, обеспечивающий идентификацию субъекта персональных данных в обезличенной базе данных с использованием уникального персонального обезличенного идентификатора физического лица;
- 4 – внешний носитель с уникальным идентифицирующим номером;
- 5 – устройство санкционирования доступа на основе устройства с SIM-картой;
- 6 – блок обработки ИСПДн2.



Система идентификации субъекта персональных данных по обезличенным данным

При обращении физического лица с целью получения услуг, он предъявляет на блок регистрации 2 информационной системы персональных данных ИСПДн1 внешний носитель 4. Система, получив уникальный идентификационный номер, сопоставляет его с записью в ОБД. Из данной записи система извлекает номер телефона устройства санкционирования доступа 5, соответствующему найденной записи и отправляет код подтверждения доступа на данный номер. Физическое лицо, получив код доступа, вводит полученный код в поле блока ввода 1. При совпадении сгенерированного кода, отправленного физическому лицу, и кода, введенного для подтверждения идентификации, субъект идентифицируется системой и ему оказывается услуга.

При необходимости определить ФИО физического лица происходит обращение к ИСПДн2 по уникальному идентификационному номеру. Блок обработки 6 ИСПДн2 используется, когда организации-оператору необходимо произвести соответствие данных пользователя с оказанными услугами. Так как подсистемы физически не связаны, то для сопоставления необходимо на накопителе перенести ОБД ИСПДн1 на блок обработки 6. Соответствие осуществляется на основе уникального идентификационного номера физического лица, который присутствует в обеих базах данных.

В случае потери или кражи идентификационного ключа злоумышленник не сможет несанкционированно воспользоваться ключом, так как у него не будет доступа к телефону, на который система отправит код подтверждения.

Предлагаемый способ идентификации субъекта персональных данных по обезличенным данным позволяет снизить вероятность использования чужого внешнего идентификатора за счет ввода в систему устройства санкционирования доступа. В случае идентификации субъекта, для проверки принадлежности внешнего носителя физическому лицу, отсылается код подтверждения на устройство санкционирования доступа. Физическое лицо вводит код подтверждения и только тогда система идентифицирует субъекта персональных данных. Применение устройства санкционирования доступа в системе позволяет достичь более высокого уровня надежности идентификации физического лица и понизить вероятность использования внешнего носителя несанкционированным пользователем системы.

При использовании данного способа идентификации субъекта персональных данных по обезличенным данным появляется возможность оказывать услуги населению без опасности кражи базы данных злоумышленником, а также позволяет организации, как оператору персональных данных, выполнять требования Федерального закона «О персональных данных» и снизить затраты организации при обработке персональных данных физических лиц за счет использования системы, обеспечивающей идентификацию субъекта персональных данных по обезличенным данным, включающую уникальный идентификационный ключ, содержащий встроенную микросхему с индивидуальным кодом, и устройство санкционирования доступа на базе устройства с SIM-картой и индивидуальным номером.

Список литературы

1. О персональных данных [Электронный ресурс] : федер. закон № 152-ФЗ : утв. Президентом Рос. Федерации 27 июля 2006 г. – Режим доступа : <http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html>. – Загл. с экрана (дата обращения: 21.05.2011).

2. Обезличивание персональных данных. [Электронный ресурс]. – Режим доступа : <http://www.sbchel.ru/personalnye-dannye/obezlichivanie-personalnykh-dannykh>. – Загл. с экрана. свободный (дата обращения: 11.08.2011)

The Method of Identification of Personal Data by Depersonalized Data

E.S. Volokitina

Southwestern State University, Kursk

Key words and phrases: authentication; information security; identification; information system of personal data; personal data; system identification; the subject of personal data.

Abstract: The paper presents the developed technique of identifying an individual using depersonalized database to comply with the requirements of the Federal Law "On Personal Data" and the cost optimization of the operator organization that processes personal data.

© Е.С. Волокитина, 2012