# БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ: НОВЫЙ ВЗГЛЯД НА СТАРУЮ ПРОБЛЕМУ

***Минзов А.С.[1] , Невский А.Ю.[2], Баронов О.Р.[3]***

***Цель статьи:*** *разработка единой модели представления персональных данных на основе решаемых в организациях задач с их использованием. Это позволяет определить минимально необходимое количество параметров в модели персональных данных при определенной вероятности решения этих задач и разработать механизм ответственности оператора персональных данных за их компрометацию.*

***Методы исследования:*** *системный анализ существующих нормативных и других документов, теория множеств и алгебра логики.*

***Результат:*** *в статье рассматриваются подходы описания модели персональных данных на основе решаемых в организациях задач, разработаны требования к совершенствованию системы защиты информации в информационных системах персональных данных (ИСПДН) и ответственности оператора персональных данных за обеспечение их конфиденциальности, целостности и доступности. Предложенная модель может быть использована в качестве методологической основы для нового подхода к решению задач по безопасной обработке, хранению, передачи ПДн.*

***Научная новизна:*** *предложен новый подход к описанию модели ПДн, основанный на решении 2-х групп задач, которые требуют применения ПДн. Определены классы угроз безопасности субъекту ПДн при компрометации данных, введено понятие «ПДн с общими групповыми признаками» и обоснована необходимость их защиты, а также сформулированы требования к системам информационной безопасности ПДн и механизмам ответственности операторов ПДн.*

***Ключевые слова:*** *информационная безопасность, модель персональных данных, угрозы, оператор персональных данных, ответственность.*

**DOI:**10.21681/2311-3456-2022-4-2-12

## Введение

Появление в Европе новой концепции защиты персональных данных в 2018 году, к сожалению, не нашло широкого отражения в отечественной печати. Хотя взгляд на систему защиты персональных данных в этой концепции несколько изменился в сторону расширения как самого понятия «персональные данные», так и в сторону создания более жестких механизмов обеспечения безопасности, контроля и ответственности операторов.

В 2006 году был принят Федеральный закон №152[4], который стал для специалистов служб информационной безопасности началом новой очень сложной работы по обеспечению требований Конституции РФ в части защиты персональных данных граждан России. За эти годы был достигнут определенный уровень понимания термина персональных данных (ПДн) и методов их защиты в информационных системах, а также отработана технология организации защиты ПДн в хозяйствующих субъектах. Наверное, можно было на этом и остановиться, но в Европе было принята новая концепция защиты ПДн GDPR (General Data Protection Regulation), которая внесла существенные и весьма значительные изме-

4 Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ (ред. от 02.07.2021) «О персональных данных».

1 Минзов Анатолий Степанович, доктор технических наук, профессор, профессор кафедры безопасности и информационных технологий национального исследовательского университета МЭИ, Москва, Россия. E-mail: MinzovAS@mpei.ru

2 Невский Александр Юрьевич, кандидат технических наук, заведующий кафедрой безопасности и информационных технологий национального исследовательского университета МЭИ, Москва, Россия. E-mail: NevskiyAU@mpei.ru

3 Баронов Олег Рюрикович, кандидат технических наук, доцент кафедры безопасности и информационных технологий национального исследовательского университета МЭИ, Москва, Россия. E-mail: BaronovOR@mpei.ru

нения в понятийный аппарат, механизмы защиты и ответственности, включая[5]:

- ***расширение понятие ПДн*** и отнесение к персональным данным информации, которая ранее не использовалась (электронные адреса, IP-адреса, метки сервера, система предпочтений пользователя при работе в сети, профили пользователей в социальных сетях и т.д.);
- ***более легкий доступ субъектов к их ПДн***, включая предоставление дополнительной информации о том, как обрабатываются эти данные;
- ***право на переносимость данных*** — изменение правил передачи персональных данных между поставщиками услуг;
- ***право на забвение*** («право на удаление персональных данных»), когда субъект ПДн больше не хочет чтобы его персональные данные обрабатывались, если для этого нет никаких законных оснований;
- ***право знать***, если данные пользователя были взломаны, что предполагает незамедлительное его информирование о нарушениях безопасности данных.

Кроме того, GDPR предоставляет простые и рабочие инструменты гражданам ЕС для реализации своих прав, упрощая механизмы обращения в надзорные органы, например, жалобы в электронном виде.

Анализ современного состояния системы защиты персональных данных показал, что этих изменений недостаточно и ряд проблем остается по-прежнему нерешенными. Среди них можно выделить следующие:

- Сохраняющееся противоречие между целями защиты ПДн и практическими результатами обеспечения их информационной безопасности. Это проявляется в том, что сегодня практически отсутствует система контроля за распространением ПДн в различных формах документов на бумажных и электронных носителях, а меры ответственности за их несанкционированное распространение весьма условны и не соответствуют потерям субъектов ПДн при компрометации их данных [1-2].
- До настоящего времени не определен круг задач, решаемых в организациях с использованием ПДн. Отсюда у администрации этих организаций возникает неуемное желание узнать о субъекте ПДн как можно больше [3].
- Расширение понятия ПДн в область «любой» информации о субъекте ПДн не нашло отражения в системе защиты информации и в самих информационных системах. Это должно было привести к появлению новых функций мониторинга и защиты ПДн в социальных сетях, поисковых системах и браузерах [4].
- Появление научных публикаций по вопросам обезличивания ПДн и обсуждение технологий реализации этих процессов не отвечают на главные вопросы: какие задачи можно решать с обезличенными данными, кто их будет решать и как контролировать эти процессы [5-7].
- В настоящее время определена ответственность операторов ПДн за несоблюдение требований обработки ПДн, которая зависит от серьезности нарушения согласно ФЗ-152, а также отдельных статей Трудового, Гражданского, Административного и Уголовного Кодексов Российской Федерации, но этого недостаточно. Требуется создание механизма определения ответственности за подобные нарушения [3].
- Отсутствие механизмов оценки достоверности ПДн может привести к существенным ошибкам в оценке действий субъекта ПДн в процессах правосудной деятельности.

Эти и другие обстоятельства натолкнули нас на определенные размышления о дальнейшем развитии системы защиты ПДн. Не все поставленные вопросы будут рассмотрены в этой статье, но мы остановимся на наиболее важных и принципиальных из них.

## 1. Сущность понятия «персональные данные

Определимся, прежде всего, с понятиями «***идентификация***» и «***аутентификация***», которые мы будем использовать в обработке персональных данных.

***Идентификация*** – это определение пользователя в автоматизированной системе по его уникальному признаку – идентификатору[6]. В роли идентификатора может выступать имя пользователя в системе (логин), числовой или буквенно-числовой код, электронная подпись, ИНН, СНИЛС, электронная почта, номер мобильного телефона или другая информация. По существу, под идентификацией понимается техническая процедура проверки принадлежности идентификатора списку или базе данных.

***Аутентификация*** – это проверка подлинности лица, которое хочет получить доступ к системе. Для

5 Общий регламент защиты персональных данных GDPR [Электронный ресурс]. URL: https://gdpr-text.com/ru/ (дата обращения: 24.06.2022).

6 ГОСТ Р 58833-2020 Идентификация и аутентификация. Общие положения

подтверждения доступа могут использоваться пароль или цифровой код (PIN-код), техническое или программное устройство (например, смарт-карта, токен, электронная подпись), или биометрические данные (например, фотография или отпечаток пальца), либо другая информация, отождествляемая с личностью человека. В том случае, если используется несколько способов подтверждения – такая аутентификация называется многофакторной.

Термин «персональные данные» определен сегодня как любая информация, относящаяся к прямо или косвенно (directly or indirectly[7]) определенному или определяемому (identified or identifiable) физическому лицу (субъекту персональных данных) (by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person)[8,9].

Весьма заметно различие в этих определениях в части выделения источников персональных данных:

- фамилия (имя) – как идентификатор;
- число – как идентификатор;
- локальные данные (отнесенные к субъекту ПДн);
- онлайновый идентификатор (IP-адрес и другие метки, относящиеся к владельцу компьютера в сети);
- информация о физиологических, психологических, интеллектуальных, экономических, культурных и социальных параметрах (идентичностей) физического лица.

Такой подход к определению ПДн, создает принципиально новый механизм защиты конфиденциальной информации, которая может различаться по трем категориям:

1. Персональные данные – это большая часть данных относящихся сегодня к другим видам тайн: банковской, страховой, налоговой, медицинской, нотариальной, усыновления, ЗАГС и еще нескольких десятков других тайн).
2. Служебная тайна.
3. Коммерческая тайна.

Первая категория (ПДн) используется в самом большом количестве информационных систем (ИСПДн) в различных сферах деятельности. Это позволяет создать единую методологию защиты информации в ИСПДн с различными уровнями защиты и ответственности операторов ПДн. Такой подход позволяет упростить систему защиты ПДн, но, с другой стороны, требует создания новых механизмов классификации уровня защищенности ИСПДн и механизмов ответственности операторов ПДн.

В последней версии ФЗ №152 вместо терминов «идентификация» и «идентифицируемый» используются термины «определенный» и «определяемый», что нарушает смысл понятия ПДн, так как не уточняет правил определения принадлежности данных к ПДн и по ФЗ №152 требует дополнительно уточнения кем и как определен набор персональных данных. При введении термина «идентифицированный» в таких дополнениях нет смысла, он определен как техническая процедура.

Остаются также неопределенными понятия «прямая» и «косвенная» информация о ПДн. Эти определения существуют в контексте понимания прямой и косвенной речи, но для ПДН они не имеют смысла, так как к ПДн относится ***любая*** информация, относящаяся к физическому лицу. Примеры ПДн также не раскрывают содержание этих терминов, так как в представленном наборе их невозможно классифицировать[10]: «Прямо или косвенно человек может быть идентифицирован с использованием идентификатора, фамилии, идентификационного номера, данных о местоположении, любые онлайн-идентификаторы, а также при помощи характерных для данного лица физических, физиологических, генетических, духовных, экономических, культурных факторов или ссылаясь на факторы социальной идентичности и т.п.». Практически понятия «прямая или косвенная» идентификация в системе защиты ПДн сегодня не используются, что также вносит неопределенность в понимание сущности ПДн.

Очень важно, что в последней версии GDPR уточнено, что данные становятся персональными, если, используя некую их совокупность, можно ***однозначно идентифицировать*** человека[11]. Термин «однозначность» имеет много синонимов, но ближе к смыслу обработки ПДн трактуется как «определенность» предъявленного набора признаков, совпадающих с одним из наборов в базе данных.

7 Курсивом выделены фрагменты этого определения в Европейском регламенте GDPR [2].

8 Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ (ред. от 02.07.2021) «О персональных данных».

9 Общий регламент защиты персональных данных GDPR [Электронный ресурс]. URL: https://gdpr-text.com/ru/ (дата обращения: 24.06.2022).

10 Общий регламент защиты персональных данных GDPR [Электронный ресурс]. URL: https://gdpr-text.com/ru/ (дата обращения: 24.06.2022).

11 Информация о GDPR на русском языке [Электронный ресурс]. URL: https://ogdpr.eu/ru (дата обращения: 25.06.2022).

Пусть $X_k$ вектор данных о субъекте ПДн, который идентифицируется в базе данных X, тогда условием однозначной идентификацией субъекта ПДн является:

$$\forall X_j, X_j \subset \boldsymbol{X}, \exists! X_j \left(X_k = X_j\right), \qquad i = \overline{1,n} \quad (1)$$

Из выражения (1) можно сделать следующий вывод: создание искусственных записей данных о владельцах ПДн может быть способом снижения требований к защищенности этих данных, так как их невозможно однозначно идентифицировать по предъявляемым наборам данных и необходимы дополнительные параметры. Отличить искусственно созданную запись от реальной в базе данных можно по дополнительному параметру – криптографической хэш-функции (*hash*), вычисляемой от идентификатора записи параметров ПДн ($a_j$) и сравнением его с заранее вычисленным значением. При этом, для искусственно созданных записей значение идентификатора $h_j$ определяется по значению ($a_j$+1). Тогда условие (1) будет иметь следующий вид:

$$\forall X_j, X_j \subset \boldsymbol{X}, \exists! X_j \left(X_k = X_j\right), \left(hash\left(a_j\right) = h_j\right) \quad i = \overline{1,n} \quad (2)$$

В выражении (2) представлен один из предложенных авторами статьи способов обезличивания данных (псевдоанонимизация) за счет создания искусственных записей в базе данных. Полный набор практических правил обезличивания приведен в работах [5-8], также в других источниках[12] и требует дальнейших исследований в части создания системы защиты и контроля безопасности ИСПДн.

Остается также невыясненным вопрос об «неоднозначной» идентификации субъекта ПДн в GDPR. Единственным объяснением появления этого термина может быть использование вероятностного подхода к идентификации субъекта ПДн. При полном совпадении предъявляемых признаков субъекта ПДН с идентифицируемыми в БД ИСПДн можно говорить об однозначной идентификации с вероятностью равной 1. В других случаях, вероятность идентификации субъекта ПДн определяется как суммарная частота (p) независимых признаков в БД ИСПДн:

$$p = 1 - \prod_{i=1}^{n} \left(1 - p_i\right) \quad (3)$$

где $p_i$ – частота идентифицируемого i-го признака в БД ИСПДн.

*p* – вероятность соответствия предъявляемых для идентификации признаков субъекту ПДн в БД ИСПДн.

Класс неоднозначно определенных ПДн достаточно широкий и очень часто мы его используем его в различных сферах деятельности, включающих: расследование инцидентов, криминалистику, деловую разведку, маркетинг, социологические исследования, судебно-правовую деятельность, PR, информационные войны и другие направления, в которых очень важны групповые, а не уникальные признаки субъектов ПДн. С точки зрения требований GDPR эти данные не относятся к ПДн и не требуют защиты. Но это далеко не так и группам субъектам ПДн с общими признаками также может быть нанесен ущерб. Значит и этот класс ПДн также требует защиты или каких-либо ограничений по сбору этих данных.

В Федеральном законе № 152 «О персональных данных» подход, основанный на понятии однозначной и неоднозначной идентификации субъекта ПДн, напрямую не рассматривается, но условие принадлежности данных определенному физическому лицу предполагает выполнения принципа однозначности (1).

Но вернемся к данным о субъекте ПДн, которые в нашем законодательстве ранее вообще не рассматривались [2]: время инициации запроса пользователем; адрес web-страницы, посещенной активным пользователем; HTTP referer (ссылка); user agent[13], coockie[14], src ip, src port, dst ip, dst port, геоидентификатор. Этот список можно продолжать техническими характеристиками компьютера субъекта ПДн, версией операционной системы, монитора, MAC – адресами оборудования сети и специализированными сведениями, собираемыми поисковыми системами по результатам запросов.

12 - Pseudonymisation techniques and best practices [Электронный ресурс]. URL: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices/@@download/fullReport (дата обращения: 02.07.2022).

- GDPR & deploying pseudonymisation techniques [Электронный ресурс]. URL: https://www.enisa.europa.eu/news/enisa-news/gdpr-deploying-pseudonymisation-techniques (дата обращения: 24.06.2022).

- Cybersecurity to the Rescue: Pseudonymisation for Personal Data Protection [Электронный ресурс]. URL: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-to-the-rescue-pseudonymisation-for-personal-data-protection (дата обращения: 24.06.2022).

- Data Pseudonymisation: Advanced Techniques and Use Cases [Электронный ресурс]. URL: https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases (дата обращения: 24.06.2022).

13 *User Agent* — это строка, которую используют веб-браузеры в качестве своего имени, она содержит не только имя браузера, но и версию операционной системы и другие параметры. По user agent можно определить достаточно много параметров, например, название операционной системы, её версию и разрядность.

14 *Cookie* — небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя

Существуют и другие, весьма чувствительные к угрозам ПДн, которые составляют огромное количество измеряемых, наблюдаемых и классифицируемых признаков:

- биометрические данные — физические, физиологические или поведенческие признаки физического лица, при помощи которых возможно однозначно идентифицировать человека. Например, изображения человеческого лица, отпечатки пальцев, сетчатки глаза, запись голоса и т.п.;
- данные о здоровье – данные о физическом или психическом здоровье человека, включающие медицинские анализы, заключения и истории болезней и другую информацию;
- генетические данные – унаследованные или приобретенные генетические признаки физического лица, предоставляющие уникальную информацию о физиологии или здоровье, а также соответствующие биологические образцы.

Кроме того, нельзя упомянуть и о другой информации, имеющей непосредственное отношение к субъекту ПДн:

- банковские счета и динамика их состояния;
- опубликованные произведения интеллектуальной собственности;
- информация, произведенная субъектом ПДн в социальных сетях и других ресурсах Интернет;
- сведения о субъекте ПДн, оставляемые в мобильных сетях, регистрирующих устройствах транспортных и других систем.

Таким образом, перечень сведений, относящихся к личности, практически неисчерпаем и может быть со временем продолжен. Каждый из признаков способен идентифицировать субъект ПДн (СПДн) с определенной вероятностью, которая может быть определена исходя из частоты этого признака в наблюдаемой выборке при условии, что этот признак имеет прямую связь с любым уникальным идентификатором личности (СНИЛС, ИНН, номер телефона мобильной связи, адрес электронной почты, реквизиты паспорта или удостоверения личности, номер личного автомобиля, водительские права и др.). Признаки личности хранятся в специально организованных базах данных, предназначенных для решения государственных, производственных, социальных, политических, культурных и других задач.

Таким образом, существующее определение не имеет точного смысла, трудно интерпретируемо, не отражает задачи и механизмы ответственности операторов обработки ПДн, что затрудняет (а практически исключает) правоприменение норм ФЗ 152 к его нарушителям. В качестве примера приведем следующее сообщение[15] «Глава Сбербанка Герман Греф уже принес извинения 200 клиентам, чьи персональные данные попали в интернет, а также всем клиентам банка за доставленные переживания. «Мы сделали серьезные выводы и кардинально усиливаем контроль доступа к работе наших систем сотрудников банка, чтобы минимизировать влияние человеческого фактора», — приводятся слова Грефа в сообщении банка». Кто оценил ущерб, нанесенный клиентам сбербанка и кто его возместил? Понятие «человеческий фактор» не применимо к системам информационной безопасности и говорит лишь о некомпетентности администрации организации.

## 2. Модель описания задач, решение которых требует использования персональных данных

Представим модель персональных данных для решения определенных задач из рассмотренного нами содержания понятия «персональные данные»:

$$N_k \rightarrow F(a_k,\ x1, x2, \dots, xn) \rightarrow Zk \mid (p \geq p_k) \qquad (4)$$

$$F^{-1}(x_1, x_2, \dots, x_n) \rightarrow a_k \rightarrow Nk \mid (p \geq pk), \qquad (5)$$

где

*Nk* – вектор параметров определенного субъекта ПДн. Этот параметр устанавливается в зависимости от решаемых социальных, экономических, политических и других задач, в которых требуется информация об этом субъекте.

$F(ak, x_1,\dots, x_n)$ – функция преобразования вектора параметров субъекта ПДн во внутреннюю форму их хранения в базе данных и назначение внутреннего идентификатора $a_k$ для задачи $Z_k$, которая решается с применением этого набора персональных данных.

$F\text{-}1(x_1,\dots, x_n)$ – обратная функция определения субъекта ПДн по предъявленным параметрам. Эта функция решает 2 задачи: определение наличия в БД предъявленных параметров (идентификация) и выдача заключения о результатах аутентификации определяемого ФЛ.

p –достоверность аутентификации по заданному набору данных для неоднозначно определенных (групповых) ПДн.

$p_k$ –требуемая достоверность решения задачи $Z_k$.

Рассмотрим подробнее классификацию параметров ПДн и решаемых задач, связанных с обработкой

15 В Сбербанке заявили о 5000 жертвах утечки данных https://www.interfax.ru/business/679460

ПДн. Параметры вектора $N_k$ с учетом уточненного значения термина ПДн в концепции GDPR [2] могут включать следующую информацию:

1. ***Внутренний идентификатор в БД*** ($a_k$).

2. ***Отраслевые идентификаторы*** (СНИЛС, ИНН, номер и серия паспорта, номер личного автомобиля, и др.). В настоящее время их количество явно избыточно для систем электронного учета[16]. Поэтому, вполне достаточно наличие единого и уникального идентификатора личности, но, желательно, по всемирной классификации. При этом предполагается, что полная информация о владельце ПДн хранится в реестре информационной системы государства, в котором владелец ПДн имеет гражданство.

3. ***Характеристики электронных идентификаторов личности*** (карты, таблетки, RFID-метки, электронный паспорт, электронная подпись, электронные идентификаторы, вживляемые в тело владельца ПДн[17]). Эти идентификаторы действуют в определенные периоды деятельности человека при решении различных задач, связанных с обработкой ПДн ($Z_k$) и обычно используются при идентификации и аутентификации личности при допуске на объект, в информационную систему или при других случаях аутентификации личности.

4. ***Признаки, сохраняющие свойства личности на длительное время, в том числе и после жизни человека*** (медицинская карта с историями заболеваний, личные дела, ДНК, социальные сети, поисковые системы, страницы сайтов и блогов с участием владельца ПДн, архивы электронной почты и мессенджеров, финансово-кредитные истории в автоматизированных банковских системах, государственные информационные системы, интеллектуальная собственность, информация о родственниках и друзьях, архивы трудовой и другой деятельности). Эти данные могут подвергаться забвению при определенных условиях[18] .

5. ***Неустойчивые признаки владельца ПДн, сохраняемые от нескольких до десятков лет*** (психофизиологические параметры личности человека и его фотографии, профили в различных информационных системах, система предпочтений при использовании ресурсов интернет и поисковых систем, информационная среда и техническое окружение человека в информационных системах, мнения, взгляды, отношения и другие реакции владельца на ситуации в информационных системах, имущественное состояние, привычки, хобби и привязанности, стиль работы в информационных системах, почтовые адреса, друзья, досье и другие выявляемые признаки).

6. ***Признаки, которые можно определить, измерить или сопоставить только в период жизни взрослого человека:*** (паспорт с биометрическими показателями личности, отпечатки пальцев, рисунок сосудов рук, радужная оболочка глаза, группа крови, рентгеновские снимки, описательные словесные портреты, телосложение, рост, размер обуви).

Параметры $N_k$ устанавливаются в зависимости от следующих решаемых задач ($Z_k$), использующих наборы признаков ПДн { $x_1$, $x_2$, ... , $x_n$ }. Нами были выделены следующие основные группы задач, список которых может быть продолжен:

1. Допустимые условия обычного прохода на территорию организации (идентификация локальная).
2. Условия регистрации при проживании в гостинице (идентификатор государственной информационной системы).
3. Идентификация проезда в транспорте (идентификатор социальный или определяющий условия проезда).
4. Идентификация и аутентификация в социальной сети и других ресурсах интернет.
5. Идентификация и аутентификация в информационных системах и АСУ.
6. Идентификация в системах контроля и управления доступом.
7. Идентификация и аутентификация в средствах доверенной загрузки.
8. Идентификация и аутентификация в системах электронной подписи (простая и усиленная).
9. Взаимодействие с органами МВД и другими ведомствами (группа задач).
10. Необходимые сведения при поступлении на обучение, работу, службу.
11. Сведения для оказания медицинских услуг (группа задач).
12. Сведения для оказания банковских услуг.
13. Сведения для оказание государственных услуг (социальных, ЗАГС и др.).
14. Сведения для регистрации при страховании.

16 Кто придумал создавать такое количество отраслевых классификаторов и во сколько обходится государству их содержание и учет ? К сожалению, на эти вопросы нет ответов.

17 Приказ Минпромэнерго РФ от 07.08.2007 №311 «Об утверждении стратегии развития электронной промышленности России на период до 2025 года», так определяет одну из перспектив развития электронных материалов и структур: «...Наноэлектроника будет интегрироваться с биообъектами и обеспечивать непрерывный контроль за поддержанием их жизнедеятельности, улучшением качества жизни, и таким образом сокращать социальные расходы государства.» [электронный ресурс] URL: https://www.roi.ru/9352/ .

18 Общий регламент защиты персональных данных GDPR [Электронный ресурс]. URL: https://gdpr-text.com/ru/ (дата обращения: 24.06.2022).

15. Сведения для получения визы.
16. Сведения для заключения договоров при сделках.
17. Сведения для электронного и обычного голосования.
18. Признаки и условия подтверждения доказательств участия субъекта ПДН в преступной деятельности (группа различных задач).

Гораздо сложнее определить значение достоверности $p_k$ . Для разных задач оно может быть различным. Например, при решении первой задачи, условие прохождения на территорию организации может быть при $p_k \geq 0{,}7$. При решении 18-й задачи достоверность совершения тяжкого преступления должна быть не ниже 0,99999. Однако, при этом, из совокупности набора признаков $F_k$ должны быть обязательно исключены те из них, распространение которых не контролируется человеком (биоматериал, отпечатки пальцев и другая информация, относящаяся к определению ДНК). Конкретно граничное значение достоверности совершения преступления должна быть определено на международном уровне обсуждения этой проблемы и может пересматриваться в зависимости от погрешностей измерения параметров признаков ПДн.

Условием решения каждой задачи ($Z_k$) является определение некоторых множеств признаков ПДн, при которых достигается выполнение задачи с вероятность не ниже заданной из всех возможных наборов данных ($n$):

$$\forall z_i,\ z_i \in Z_k,\ \exists (N_i \mid p_i \geq p_k),\ \text{при } i = 1..n. \qquad (6)$$

Конкретное содержание этого набора данных определяется нормативным актом государства, ведомства или организации. Однако, чем выше значение вероятности решения задачи идентификации владельца ПДн, тем выше и ответственность этой организации за безопасность сохранения ПДн. Конкретные значения ответственности операторов обработки ПДн определяются угрозами личности в зависимости от набора данных, которые были скомпрометированы (опубликованы без согласия владельца, похищены и использованы в мошеннических целях). В настоящее время в научной среде эти вопросы практически не обсуждаются.

### 3. Классификация угроз безопасности персональным данным для человека

К сожалению, базовая модель угроз ПДн[19] и методические рекомендации[20] не рассматривают угрозы личности, хотя это может привести к более глубокому пониманию методов защиты ПДн, которые потребуют принятия определенных организационных и технических решений, не предусмотренных существующими нормативными документами[21,22] . Выделим наиболее важные угрозы безопасности для субъекта ПДН [8]:

1. Фальсификация субъекта ПДн путем использования поддельных документов.
2. Шантажирование субъекта ПДн открытыми публикациями компрометирующего характера.
3. Психологическое давление постоянными атаками на субъекта ПДн с целью принуждения и манипулирования (троллинг).
4. Сбор сведений о системах предпочтений субъекта ПДн.
5. Сбор сведений о геолокации субъекта ПДн.
6. Компрометация субъекта ПДн путем публикаций аудио и видео записей с личной (частной) информацией.
7. Выполнение несанкционированных действий от имени субъекта ПДн.
8. Изменение документов субъекта ПДн.
9. Захват недвижимости субъекта ПДн при фальсификации документов.
10. Овладение счетами субъекта ПДн применением методов социальной инженерии.
11. Подмена (фальсификация) биологических образцов субъекта ПДн.
12. Подлог на месте преступления свидетельств субъекта ПДн.
13. Манипуляция общественным мнением в отношении субъекта ПДн.
14. Раскрытие личной и семейной тайны.
15. Добывание личной информации методами социальной инженерии.
16. Получение доступа к ключам электронной подписи и использования их в личных целях.
17. Использование технических средств (снифферы) для контроля трафика сообщений (мессенджеров, электронной почты и передаваемых файлов).
18. Создание ложной системы доказательств проявления активности пользователя в сети.
19. Создание фантомов (профилей пользователей) в социальных сетях с компрометирующей информацией.

19 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год.

20 Методика оценки угроз безопасности информации. ФСТЭК России, 05.022.2022

21 Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

22 Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

20. Атака на репутацию цели.
21. Нанесение ущерба здоровью цели атаки.
22. Нанесение ущерба близким и родным цели.
23. Создание напряженности, паники у группы лиц, объединенных по национальным, территориальным или социальным групповым признакам.
24. Распространение компрометирующих слухов по групповым признакам.
25. Выполнение несанкционированных действий от имени субъекта ПДн.

Практически все эти угрозы реализуются на полной или частичной открытости ПДН, которая может произойти как по вине самого субъекта ПДн, так и при плохой защите ПДН по вине оператора обработки ПДн. В последнем случае необходимо учитывать эти угрозы в модели ответственности оператора ПДн.

## 4. Требования к системе управления персональными данными и ответственности за их обработку

Исходя из изложенных нами моделей представления ПДн, решаемых задач и угроз субъектам ПДн уровень их защищенности в системах обработки должен определяться:

1. Количеством параметров в принятой организацией модели ПДн ($N_k$) и решаемых в ИСПДн задач ($Z_k$). Чем больше параметров в принятой модели ПДн в организации, тем больше уровень защищенности ИСПДн.
2. Характером угроз владельцам ПДн при компрометации данных, содержащихся о них в БД ИСПДн. Чем больше угроз может быть реализовано, тем выше уровень защищенности ИСПДн.
3. Требованиями по достоверности аутентификации владельцев ПДн ($p_k$). Это требование определяется тем, что в БД ИСПДН, в которых проводится обработка неоднозначно классифицируемых записей ПДн с определенными общими групповыми признаками, могут быть реализованы групповые угрозы. Масштабы этих угроз зависят от объемов БД ИСПДн, способов группирования выборок субъектов ПДн и модели угроз.
4. Полным набором защитных мероприятий, включающих меры по локализации обработки ПДн, контроля за их распространением и расследованием инцидентов. Существующие требования по защите информации в ИСПДН не содержат полный набор мероприятий по защите ИСПДН, в том числе [11,12,13]:
   - по требованиям к архитектуре ИСПДН, позволяющей локализовать обработку ПДн в защищенной среде;
   - по организации системы защиты ПДн на всех этапах их обработки:
   - по контролю за распространением и уничтожением информации о ПДн в различных формах их представления.
5. Соответствующей моделью ответственности организации за обработку ПДн.

Уровень ответственности за компрометацию, искажение или передачу информации о ПДн должен определяться:

1. Количеством параметров в принятой организацией модели ПДн (Nk) для решения разных задач.
2. Количеством владельцев ПДн (числом записей в базе данных).
3. Модели угроз, которые могут быть реализованы для владельцев ПДн.
4. Величиной параметра экономической эффективности или бюджета организации для определения максимального уровня штрафных санкций при инцидентах информационной безопасности, связанных с компрометацией ПДн.

## Заключение

- Современное определение ПДн трактует практически все ИС, имеющие персональные данные, как информационные системы ПДн (ИСПДн).
- Обе задачи (4,5) имеют вероятностный смысл. Это означает, что достичь определенную вероятность аутентификации возможно большим количеством «слабых» признаков или/и уменьшением множества объектов в базе данных.
- Если первая задача (4) не может быть точно определена, то вторая задача (5) должна иметь конкретные критерии решения задачи аутентификации физического лица (при устройстве на работу, при допуске к конфиденциальной информации, при определении полноты улик и т.д.).
- Рассмотренные требования к защите ПДн ориентирована на угрозы физическому лицу и могут быть использована при выборе модели ПДн для решения конкретной задачи.
- Предложенные требования к системе защиты ПДн стимулируют организации, проводящие обработку ПДн, к уменьшению количества параметров в модели данных и созданию системы контроля за их распространением.

— Технологии больших данных [9, 14] и использование различных источников информации [10, 15] практически могут свести к нулю усилия по обезличиванию ПДн. Это потребует введения новых технологий контроля ответственности операторов ПДн за распространение БД с ПДн.
— Существующие мнения о необходимости введения полного контроля в Интернете за счет отсутствия анонимности пользователей [11] не совпадают с мнением авторов этой статьи и не соответствует тенденциям развития информационных систем. Это возможно только при решении специальных задач по постановлению судебных органов. Необходимость анонимности ПДн должна регулироваться самим субъектом ПДн, а уровень защищенности этих данных должен определяться оценками рисков [12] и моделью ответственности оператора ПДн.

**Литература**


1. Солдатова В.И. Защита персональных данных в условиях применения цифровых технологий. Lex russica (Русский закон). 2020;73(2). С.33-43. https://doi.org/10.17803/1729-5920.2020.159.2.033-043
2. Мочалов А. Н. Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности // Lex russica. — 2021. — Т. 74. — № 9. — С. 88–101. — DOI: 10.17803/1729-5920.2021.178.9.088-101.
3. Chris Jay Hofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius (2019) European Union General Data Protection Regulation: What it is and what it means, Information and Communications Technology Act, 28:1, 65-98, DOI: 10.1080/ 13600834.2019 .1573501
4. Чехарина В. И. О конституционализации права на защиту персональных данных: из зарубежного опыта // Международный журнал гуманитарных и естественных наук. – 2020. – №. 3-2. – С. 223-228.
5. Харитонова А. Р. Сохранность и анонимность персональных данных в социальных сетях // Предпринимательское право. Приложение» Право и Бизнес». – 2019. – №. 4. – С. 48-55. eLIBRARY ID: 41321580
6. Кузнецова С. С. Право на анонимность в сети Интернет: актуальные вопросы реализации и защиты // Российское право: образование, практика, наука. 2020. № 5. С. 33–41. DOI: 10.34076/2410-2709-2020-5-33-41
7. Карцхия А. А. Тенденции развития правовых институтов под влиянием пандемии: российский и зарубежный опыт // Мониторинг правоприменения. – 2021. – №. 1 (38). – С. 10-15. DOI:10.21681/2226-0692-2021-1-10-15
8. Докучаев В. А., Маклачкова В. В., Статьев В. Ю. Классификация угроз безопасности персональных данных в информационных системах // T-Comm - Телекоммуникации и Транспорт.– 2020. № 1
9. Рожкова М. А., Глонина В. Н. Персональные и неперсональные данные в составе больших данных // Право цифровой экономики–2020. Ежегодник-антология/рук. и науч. ред. МА Рожкова. Москва: Статут. – 2020. – С. 271-296.
10. Ingo Siegert, Vered Silber Varod, Nehoray Carmi, Pawel Kamocki (2020) Personal data protection and academia: GDPR issues and multi-modal datacollections «in the wild»\ Article in Online Journal of Applied Knowledge Management • June 2020. DOI: 10.36965/OJAKM.2020.8(1)16-31
11. Смоленский М. Б., Левшин Н. С. Законодательство о персональных данных как инструмент государственного регулирования в сфере информационных коммуникаций // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2019. – №. 5. – С. 75-80.
12. Моделирование рисков информационной безопасности в цифровой экономике: монография / А.С. Минзов, Е.Н. Черемисина, Н.А. Токарева, С.В. Бобылева; под ред. А.С. Минзова. — М.: КУРС, 2021. — 112 с.
13. Станкевич М.А., Игнатьев Н.А., Смирнов И.В., Кисельникова Н.В. Выявление личностных черт у пользователей социальной сети ВКонтакте // Вопросы кибербезопасности. 2019. № 4 (32). С. 80-87. DOI: 10.21681/2311-3456-2019-4-80-87
14. Кондаков С.Е., Чудин К.С. Разработка исследовательского аппарата оценки эффективности мер обеспечения защиты персональных данных // Вопросы кибербезопасности. 2021. № 5 (45). С. 45-51. DOI: 10.21681/2311-3456-2021-5-45-51
15. Дорофеев А.В., Марков А.С. Структурированный мониторинг открытых персональных данных в сети интернет // Мониторинг правоприменения. 2016. № 1 (18). С. 41-53.

# SECURITY OF PERSONAL DATA: A NEW LOOK AT THE OLD PROBLEM

*Minzov A.S[23]. , Nevsky A.Yu[24]. , Baronov O.R.[25]*

*The emergence in Europe of a new concept of personal data (PD) protection in 2018 did not find wide coverage in the domestic press. The PD protection system in this concept has changed somewhat in the direction of expanding both the very concept of "personal data", and in the direction of creating strict mechanisms for ensuring and controlling security.*

***The purpose of the article**: the development of a unified model for the presentation of PD to solve certain problems.*

*This allows you to determine the minimum required number of parameters in the PD model with a certain probability of solving these problems and develop a mechanism for responsibility for their processing.*

*The proposed model can be used as a novel approach to solving the problems of secure processing, storage, transfer and liability.*

***Main research methods**: system analysis of existing normative and other documents, set theory and algebra of logic.*

***Scientific novelty**. A new approach to the description of the PD model is proposed, based on the solution of 2 groups of tasks that require the use of this data. The classes of security threats to the subject of PD in case of their compromise are determined. Requirements for information security systems and mechanisms of responsibility of personal data operators are formulated.*

***Keywords:** information security, personal data model, threats, personal data operator, responsibility, GDPR.*

**References**

1. Soldatova V.I. Zashhita personal'nyh dannyh v uslovijah primenenija cifrovyh tehnologij. Lex russica (Russkij zakon). 2020;73(2). S.33-43. https://doi.org/10.17803/1729-5920.2020.159.2.033-043
2. Mochalov A. N. Cifrovoj profil': osnovnye riski dlja konstitucionnyh prav cheloveka v uslovijah pravovoj neopredelennosti // Lex russica. — 2021. — T. 74. — № 9. — S. 88–101. — DOI: 10.17803/1729-5920.2021.178.9.088-101.
3. Chris Jay Hofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius (2019) European Union General Data Protection Regulation: What it is and what it means, Information and Communications Technology Act, 28:1, 65-98, DOI: 10.1080/ 13600834.2019 .1573501
4. Cheharina V. I. O konstitucionalizacii prava na zashhitu personal›nyh dannyh: iz zarubezhnogo opyta //Mezhdunarodnyj zhurnal gumanitarnyh i estestvennyh nauk. – 2020. – №. 3-2. – S. 223-228.
5. Haritonova A. R. Sohrannost› i anonimnost› personal›nyh dannyh v social›nyh setjah //Predprinimatel›skoe pravo. Prilozhenie» Pravo i Biznes». – 2019. – №. 4. – S. 48-55.
6. Kuznecova S. S. Pravo na anonimnost› v seti Internet: aktual›nye voprosy realizacii i zashhity // Rossijskoe pravo: obrazovanie, praktika, nauka. 2020. № 5. S. 33–41. DOI: 10.34076/2410-2709-2020-5-33-41
7. Karchija A. A. Tendencii razvitija pravovyh institutov pod vlijaniem pandemii: rossijskij i zarubezhnyj opyt //Monitoring pravoprimenenija. – 2021. – №. 1 (38). – S. 10-15.
8. Dokuchaev V. A., Maklachkova V. V., Stat›ev V. Ju. Klassifikacija ugroz bezopasnosti personal›nyh dannyh v informacionnyh sistemah // T-Comm - Telekommunikacii i Transport.– 2020. № 1
9. Rozhkova M. A., Glonina V. N. Personal›nye i nepersonal›nye dannye v sostave bol›shih dannyh // Pravo cifrovoj jekonomiki–2020. Ezhegodnik-antologija/ruk. i nauch. red. MA Rozhkova. Moskva: Statut. – 2020. – S. 271-296.

23 Anatoly S. Minzov, Dr.Sc., Professor of the Department of Security and Information Technologies, National Research University MPEI, Moscow, Russia. E-mail: MinzovAS@mpei.ru

24 Alexander Yu. Nevsky, Ph.D., Head of the Department of Security and Information Technologies, National Research University MPEI, Moscow, Russia. E-mail: NevskiyAU@mpei.ru

25 Oleg R. Baronov, Ph.D., Associate Professor of the Department of Security and Information Technologies, National Research University MPEI, Moscow, Russia.E-mail: BaronovOR@mpei.ru

10. Ingo Siegert, Vered Silber Varod, Nehoray Carmi, Pawel Kamocki (2020) Personal data protection and academia: GDPR issues and multi-modal datacollections «in the wild»\ Article in Online Journal of Applied Knowledge Management · June 2020. DOI: 10.36965/OJAKM.2020.8(1)16-31
11. Smolenskij M. B., Levshin N. S. Zakonodatel›stvo o personal›nyh dannyh kak instrument gosudarstvennogo regulirovanija v sfere informacionnyh kommunikacij // Nauka i obrazovanie: hozjajstvo i jekonomika; predprinimatel›stvo; pravo i upravlenie. – 2019. – №. 5. – S. 75-80.
12. Modelirovanie riskov informacionnoj bezopasnosti v cifrovoj jekonomike: monografija / A.S. Minzov, E.N. Cheremisina, N.A. Tokareva, S.V. Bobyleva; pod red. A.S. Minzova. — M.: KURS, 2021. — 112 s.
13. Stankevich M.A., Ignat'ev N.A., Smirnov I.V., Kisel'nikova N.V. Vyjavlenie lichnostnyh chert u pol'zovatelej social'noj seti VKontakte // Voprosy kiberbezopasnosti. 2019. № 4 (32). S. 80-87. DOI: 10.21681/2311-3456-2019-4-80-87
14. Kondakov S.E., Chudin K.S. Razrabotka issledovatel'skogo apparata ocenki jeffektivnosti mer obespechenija zashhity personal'nyh dannyh // Voprosy kiberbezopasnosti. 2021. № 5 (45). S. 45-51. DOI: 10.21681/2311-3456-2021-5-45-51
15. Dorofeev A.V., Markov A.S. Strukturirovannyj monitoring otkrytyh personal'nyh dannyh v seti internet // Monitoring pravoprimenenija. 2016. № 1 (18). S. 41-53.