МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ ISO/IEC 29100— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основы защиты персональных данных

(ISO/IEC 29100:2011, Information technology — Security techniques — Privacy framework, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

Цели, основные принципы и общие правила проведения работ по межгосударственной стандартизации установлены ГОСТ 1.0 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены»

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН), Акционерным обществом «Аладдин Р.Д.» (АО «Аладдин Р.Д.») и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 5

2 ВНЕСЕН Федеральным агентством по техническому регулированию и метрологии

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 30 июня 2021 г. № 141-П)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004—97	Код страны по МК (ИСО 3166) 004—97	Сокращенное наименование национального органа по стандартизации
Армения	AM	ЗАО «Национальный орган по стандартизации и метрологии» Республики Армения
Беларусь	BY	Госстандарт Республики Беларусь
Киргизия	KG	Кыргызстандарт
Россия	RU	Росстандарт
Узбекистан	UZ	Узстандарт

4 Приказом Федерального агентства по техническому регулированию и метрологии от 2 июня 2021 г. № 610-ст межгосударственный стандарт ISO/IEC 29100—2021 введен в действие в качестве национального стандарта Российской Федерации с 30 ноября 2021 г.

5 Настоящий стандарт идентичен международному стандарту ISO/IEC 29100:2011 «Информационные технологии. Методы и средства обеспечения безопасности. Основы приватности» («Information technology — Security techniques — Privacy framework», IDT), включая изменения Amd.1:2018.

Изменения к указанному международному стандарту, принятые после его официальной публикации, внесены в текст настоящего стандарта и выделены двойной вертикальной линией, расположенной на полях напротив соответствующего текста, а обозначение и год принятия изменения приведены в скобках после соответствующего текста (в примечании к тексту).

ISO/IEC 29100:2011 разработан подкомитетом SC 27 «Методы и средства обеспечения безопасности ИТ» Совместного технического комитета JTC 1 «Информационные технологии» Международной организации по стандартизации (ISO) и Международной электротехнической комиссии (IEC).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ 1.5 (подраздел 3.6).

Дополнительные сноски в тексте стандарта, выделенные курсивом, приведены для пояснения текста оригинала

6 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории указанных выше государств публикуется в указателях национальных стандартов, издаваемых в этих государствах, а также в сети Интернет на сайтах соответствующих национальных органов по стандартизации.

В случае пересмотра, изменения или отмены настоящего стандарта соответствующая информация будет опубликована на официальном интернет-сайте Межгосударственного совета по стандартизации, метрологии и сертификации в каталоге «Межгосударственные стандарты»

Содержание

Введение

Настоящий стандарт предоставляет высокоуровневые основы обеспечения безопасности персональных данных (ПДн) в информационных системах персональных данных. Стандарт является общим по своему характеру, определяет место организационных, технических и процедурных аспектов в общей структуре обеспечения безопасности персональных данных.

Общие принципы обеспечения безопасности ПДн предназначены для содействия организациям в определении требований к мерам защиты ПДн в информационных системах персональных данных посредством:

- продвижения общей терминологии, связанной с обеспечением безопасности ПДн;
- определения субъектов и их ролей при обработке ПДн;
- описания требований к мерам обеспечения безопасности ПДн;
- использования ссылок на известные основы обеспечения безопасности ПДн.

В некоторых странах положения настоящего стандарта, связанные с мерами защиты ПДн, могут расцениваться как уточнение и дополнение к законодательным требованиям обеспечения безопасности ПДн[1)]. Из-за растущего числа информационно-коммуникационных технологий (ИКТ), которые обрабатывают ПДн, важно применять стандарты по информационной безопасности, которые обеспечивают общее понимание защиты ПДн. Настоящий стандарт предназначен для улучшения существующих стандартов безопасности за счет акцентирования внимания на обработке персональных данных.

Увеличение коммерческого использования и ценности ПДн, совместного применения ПДн разными странами, а также растущая сложность информационных систем персональных данных могут затруднить для организации обеспечение безопасности ПДн и соответствие нормативным правовым актам. Лица, заинтересованные в обеспечении безопасности ПДн, могут предотвратить возникновение неуверенности и недоверия посредством надлежащего обращения с ПДн, а также избегая случаев нарушения типовых правил обработки ПДн.

Использование настоящего стандарта призвано:

- содействовать проектированию, реализации, эксплуатации и поддержке систем, которые обрабатывают ПДн при условии обеспечения их защиты;
- стимулировать инновационные решения, позволяющие обеспечивать безопасность ПДн в информационных системах персональных данных;
- совершенствовать корпоративные программы обеспечения безопасности ПДн благодаря использованию лучших практических приемов.

Основы обеспечения безопасности ПДн, представленные в настоящем стандарте, могут служить базой для дополнительных инициатив по стандартизации безопасности ПДн, таких как:

- применение базовой технической архитектуры;
- реализация и использование конкретных технологий обеспечения безопасности ПДн и общего управления защитой ПДн;
- применение мер обеспечения безопасности ПДн для процессов обработки данных в рамках аутсорсинга;
- оценка рисков нарушения безопасности ПДн;
- использование определенных технических спецификаций.

Некоторые страны могут потребовать соответствия с одним или несколькими нормативными документами, на которые имеются ссылки в постоянно действующем документе ISO/IEC JTC 1/SC 27 WG 5 «Standing Document 2 (WG 5 SD2) — Official Privacy Documents References» («Библиографический список официальных документов по защите ПДн») [3], или с другими соответствующими законами и нормативными документами, но использование настоящего стандарта в качестве основы для разработки глобальной стратегии или законодательных основ не предусматривается (Изменение Amd.1:2018).

---

1) *Настоящий стандарт необходимо применять с учетом требований национальных нормативных правовых актов и стандартов в области защиты информации стран Содружества Независимых Государств.*

Федеральное агентство
по техническому регулированию
и метрологии
Федеральное агентство
по техническому регулированию
и метрологии

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основы защиты персональных данных

Information technology. Security techniques. Privacy protection fundamentals

Дата введения — 2021—11—30

1 Область применения

В настоящем стандарте представлены основы обеспечения безопасности персональных данных (ПДн), которые:

- устанавливают общую терминологию в области безопасности ПДн;
- определяют субъектов и их роли в обработке ПДн;
- описывают концепции безопасности ПДн;
- предоставляют ссылки на методы обеспечения безопасности ПДн.

Настоящий стандарт предназначен для физических лиц и организаций, вовлеченных в определение особенностей, приобретение, моделирование, проектирование, создание, тестирование, обслуживание, управление и функционирование систем ИКТ или услуг, для которых при обработке ПДн требуются меры обеспечения безопасности ПДн.

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

Примечание — В целях упрощения использования семейства стандартов ISO/IEC 27000 в специфическом контексте безопасности ПДн и интеграции понятий безопасности ПДн в контексте ISO/IEC 27000 в таблице, приведенной в приложении А, представлены понятия по ISO/IEC 27000, соответствующие понятиям, используемым в настоящем стандарте.

2.1 **анонимность** (anonymity): Свойство информации, не позволяющее прямо или косвенно определить субъекта ПДн.

2.2 **обезличивание** (anonymization): Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

2.3 **обезличенные данные** (anonymized data): Данные, которые были получены в результате процесса обезличивания ПДн.

2.4 **согласие** (consent): Добровольное, конкретное и осознанное разрешение, данное субъектом ПДн на обработку его ПДн.

2.5 **идентифицируемость** (identifiability): Условие, результатом которого является прямая или косвенная идентификация субъекта ПДн на основе данного набора ПДн.

2.6 [Исключен] (Изменение Amd.1:2018).

2.7 [Исключен] (Изменение Amd.1:2018).

Издание официальное

2.8 **согласие на обработку** (opt-in): Процесс или тип политики, посредством которой субъект ПДн обязан предпринять действие, чтобы выразить определенное, ясное и заблаговременное согласие на обработку его ПДн для конкретной цели.

Примечание — Другим термином, часто используемым в отношении защиты ПДн в рамках принципа «согласие и выбор», является термин «запрет на обработку». С его помощью описывается процесс или тип политики, посредством которой субъект ПДн обязан предпринять отдельное действие, чтобы отказать или отозвать согласие либо воспрепятствовать осуществлению определенного вида обработки его ПДн. Использование политики отказа от обработки предполагает, что оператор ПДн обладает правом обработки ПДн назначенным образом. Под этим правом может подразумеваться некое действие субъекта ПДн, отличающееся от согласия (например, размещение заказа в онлайн-магазине).

2.9 **персональные данные** (personally identifiable information, ПДн): (a) Любая информация, с помощью которой может быть установлена связь между этой информацией и личностью (физическим лицом) того, к кому относится эта информация; (b) информация, которая прямо или косвенно может быть отнесена к определяемому физическому лицу.

Примечание — Для того чтобы определить, является ли субъект ПДн (2.11) идентифицируемым, следует учесть все средства, которые могут быть корректно использованы лицом, заинтересованным в обеспечении безопасности ПДн, владеющим данными, или любой другой стороной для идентификации этого физического лица.

(Изменение Amd.1:2018.)

2.10 **оператор ПДн** (PII controller): Государственные органы, муниципальные органы, юридические или физические лица, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, определяющие цели и состав подлежащих обработке ПДн, а также действия (операции), совершаемые с ПДн.

Примечание — Оператор ПДн может давать указания другим (например, третьей стороне) по обработке ПДн от своего лица, в то время как ответственность за обработку остается за оператором ПДн.

2.11 **субъект ПДн** (PII principal): Физическое лицо, к которому относятся ПДн.

Примечание — В зависимости от страны и конкретного закона в области защиты данных и обеспечения защиты ПДн вместо термина «субъект ПДн» может быть использован синоним «субъект данных».

2.12 **обработчик ПДн** (PII processor): Лицо, заинтересованное в обеспечении защиты ПДн, которое обрабатывает ПДн от имени и в соответствии с инструкциями оператора ПДн.

2.13 **нарушение безопасности ПДн** (privacy breach): Ситуация, когда ПДн обрабатываются в нарушение одного или более соответствующих требований обеспечения безопасности ПДн.

2.14 **меры обеспечения безопасности ПДн** (privacy controls): Меры, которые в соответствии с законодательством принимаются для защиты ПДн.

Примечания

1 Меры обеспечения безопасности ПДн включают в себя организационные, физические и технические меры, например политики, процедуры, рекомендации, законные контракты, практики менеджмента или организационные структуры.

2 Термин «меры обеспечения безопасности ПДн» также применяется как синоним защитных мер или контрмер.

2.15 **технология, улучшающая защищенность ПДн** (privacy enhancing technology, PET): Меры обеспечения безопасности ПДн, состоящие из мер, продуктов или сервисов информационной системы персональных данных, которые обеспечивают защиту ПДн путем уничтожения или сокращения объема ПДн, или предотвращения ненужной и (или) нежелательной обработки ПДн без потери функциональности информационной системы персональных данных.

Примечания

1 Примерами использования PET являются средства обезличивания и применения псевдонимов, которые устраняют, уменьшают, маскируют или обезличивают ПДн либо предотвращают ненужную, несанкционированную и (или) нежелательную обработку ПДн, но не ограничиваются ими.

2 Маскирование является процессом, в результате которого происходит затруднение понимания ПДн.

2.16 **политика обеспечения защиты ПДн** (privacy policy): Общее намерение и направление деятельности, правила и обязательства, формально выраженные оператором ПДн, касающиеся обработки ПДн в определенной области.

2.17 **предпочтительные способы обеспечения защиты ПДн** (privacy preferences): Конкретный выбор, сделанный субъектом ПДн в отношении того, как должны быть обработаны для определенной цели его ПДн.

2.18 **принципы обеспечения защиты ПДн** (privacy principles): Совокупность утверждений, направленных на управление обеспечением защиты ПДн при их обработке в информационных системах персональных данных.

2.19 **риск нарушения безопасности ПДн** (privacy risk): Вероятность нарушения безопасности ПДн.

Примечания

1 В ISO Guide 73 и ISO 31000 риск определяется как «влияние неопределенности на цели».

2 Неопределенность — это состояние, даже частичное, отсутствия информации, касающейся понимания или знания о событии, его последствиях или вероятности.

2.20 **оценка негативных последствий (оценка риска) нарушения безопасности ПДн** (privacy impact assessment, PIA, privacy risk assessment): Общий процесс идентификации, анализа и оценки риска и возможных негативных последствий нарушения безопасности ПДн, включая необходимые элементы консультирования, обсуждения и планирования соответствующих мер противодействия, согласованных с общей политикой менеджмента рисков организации.

[ISO/IEC 29134:2019, статья 3.7 с изменениями — добавлен термин «оценка риска нарушения безопасности ПДн»]

(Изменение Amd.1:2018).

2.21 **требования к мерам обеспечения безопасности ПДн** (privacy safeguarding requirements): Набор требований, которые организация должна учитывать при обработке ПДн в части обеспечения безопасности ПДн.

2.22 **лицо, заинтересованное в обеспечении безопасности ПДн** (privacy stakeholder): Физическое или юридическое лицо, орган государственной власти, агентство или какая-либо другая организация, которые могут влиять, подвергаться влиянию или испытывать на себе влияние решения или деятельности, связанной с обработкой ПДн.

2.23 **обработка ПДн** (processing of PII): Любая операция или совокупность операций, выполняемых в отношении ПДн.

Примечание — Примерами операций являются (но не ограничиваются этим): любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение ПДн.

2.24 **применение псевдонима** (pseudonymization): Процесс, относящийся к ПДн, который заменяет идентификационную информацию псевдонимом.

Примечания

1 Замена идентификационной информации субъекта псевдонимом может выполняться либо самими субъектами ПДн, либо операторами ПДн. Такая замена может быть использована субъектами ПДн для последовательного применения ресурса или сервиса без раскрытия своей идентификационной информации в отношении данного ресурса или сервиса (или между сервисами), при этом они несут ответственность за это использование.

2 Замена идентификационной информации субъекта псевдонимом не исключает возможность существования ограниченного числа лиц, заинтересованных в обеспечении защиты ПДн, не являющихся операторами ПДн псевдонимных данных, но способных определять идентификационную информацию о субъектах ПДн, основываясь на псевдонимах и связанных с ними данных.

2.25 **вторичное использование** (secondary use): Обработка ПДн в условиях, отличающихся от начальных условий.

Примечание — Условия, отличающиеся от начальных условий, могут включать в себя, например, новую цель обработки ПДн, нового получателя ПДн и т. п.

2.26 **специальные категории ПДн** (sensitive PII): Категория ПДн, которая либо является по своей природе чувствительной информацией, например затрагивает наиболее личную сферу субъекта ПДн, либо может оказывать нежелательное воздействие на персональные данные субъекта ПДн.

Примечание — В некоторых странах или при определенных обстоятельствах специальные категории ПДн определяются относительно типа ПДн и могут состоять из ПДн, раскрывающих расовую принадлежность, политические убеждения или религиозные верования, персональные данные о здоровье, сексуальной жизни или преступлениях, и других ПДн, которые могут быть определены как чувствительная к разглашению информация.

2.27 **третья сторона** (third party): Лицо, заинтересованное в обеспечении защиты ПДн, не являющееся субъектом ПДн, оператором ПДн или обработчиком ПДн, а также физические лица, уполномоченные обрабатывать данные под непосредственным руководством оператора ПДн или обработчика ПДн.

3 Сокращения

В настоящем стандарте применены следующие сокращения:

PET — технология, улучшающая защищенность ПДн (privacy enhancing technology);

ИКТ — информационно-коммуникационные технологии (information and communication technology);

ПДн — персональные данные (personally identifiable information).

4 Основные элементы защиты персональных данных

4.1 Общий обзор защиты персональных данных

Следующие компоненты связаны с обеспечением защиты ПДн и обработкой ПДн в информационных системах персональных данных и составляют основы обеспечения защиты ПДн, описанные в настоящем стандарте:

- субъекты и роли;
- взаимодействие;
- распознавание ПДн;
- требования к мерам обеспечения безопасности ПДн;
- политики обеспечения безопасности ПДн;
- меры обеспечения безопасности ПДн.

При разработке основ обеспечения защиты ПДн учитывались понятия, определения и рекомендации из других официальных источников. Информация об указанных источниках содержится в постоянно действующем документе ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 «Official Privacy Documents References» («Библиографический список официальных документов по защите ПДн») [3].

4.2 Субъекты и роли

Для целей настоящего стандарта важно идентифицировать субъектов, вовлеченных в обработку ПДн. Существуют четыре типа субъектов, которые могут быть вовлечены в обработку ПДн: субъекты ПДн, операторы ПДн, обработчики ПДн и третьи стороны.

4.2.1 Субъекты персональных данных

Субъекты ПДн предоставляют свои ПДн для обработки операторам ПДн и обработчикам ПДн и, если обратное не установлено применимым законодательством, они дают согласие и определяют свои предпочтения в отношении способов обработки их ПДн. Например, субъектом ПДн может быть работник, включенный в штатное расписание организации, или потребитель, упомянутый в отчете о кредитных операциях, или пациент, запись о здоровье которого внесена в электронную базу. Чтобы считаться субъектом ПДн, соответствующее физическое лицо необязательно должно быть идентифицировано по его имени. Если физическое лицо, к которому относятся ПДн, может быть идентифицировано косвенно (например, через идентификатор счета, номер полиса социального страхования или даже через комбинацию доступных признаков), оно также является субъектом ПДн для данного набора ПДн.

4.2.2 Операторы персональных данных

Оператор ПДн определяет, почему (цель) и как (способы) обрабатываются ПДн. В данной структуре оператор ПДн должен обеспечивать уверенность в том, что соблюдение принципов защиты ПДн во

время обработки ПДн осуществляется под его контролем (например, путем реализации необходимых мер обеспечения безопасности ПДн). Может существовать более одного оператора ПДн для одного и того же набора ПДн или набора операций, выполняемых в отношении ПДн (для тех же самых или различных легальных целей). В этом случае операторы ПДн должны сотрудничать и обеспечивать выполнение принципов обеспечения безопасности ПДн во время обработки ПДн. Оператор ПДн также может разрешить выполнение всех или части операций по обработке ПДн другим лицам, заинтересованным в обеспечении защиты ПДн, от своего лица. Операторы ПДн должны тщательно оценивать, обрабатывают они чувствительную (специальные категории ПДн) или нечувствительную информацию, и реализовывать рациональные меры обеспечения безопасности ПДн на основе требований, установленных в соответствующей стране, а также оценивать любое возможное негативное влияние на субъектов ПДн в связи с их идентификацией во время оценки риска обеспечения защиты ПДн.

4.2.3 Обработчики персональных данных

Обработчик ПДн выполняет обработку ПДн от имени оператора ПДн, действует от имени или в соответствии с инструкциями оператора ПДн, соблюдает установленные требования обеспечения защиты ПДн и реализует соответствующие меры обеспечения безопасности ПДн. В некоторых странах обработчик ПДн ограничен законным договором.

4.2.4 Третьи стороны

Третья сторона может получать ПДн от оператора ПДн или обработчика ПДн. Третья сторона не обрабатывает ПДн от имени оператора ПДн. В основном третья сторона становится самостоятельным оператором ПДн после получения запрашиваемых ПДн.

4.3 Взаимодействия

Субъекты, идентифицированные в 4.2, могут взаимодействовать между собой различным образом. Можно идентифицировать следующие сценарии, формирующие потоки ПДн между субъектом ПДн, оператором ПДн и обработчиком ПДн:

a) субъект ПДн предоставляет ПДн оператору ПДн (например, регистрация для оказания услуги оператором ПДн);

b) оператор ПДн предоставляет ПДн обработчику ПДн, который обрабатывает эти ПДн от имени оператора ПДн (например, как часть соглашения об аутсорсинге);

c) субъект ПДн предоставляет ПДн обработчику ПДн, который обрабатывает эти ПДн от имени оператора ПДн;

d) оператор ПДн предоставляет ПДн субъекту ПДн, и они относятся к субъекту ПДн (например, в соответствии с запросом, сделанным субъектом ПДн);

e) обработчик ПДн предоставляет ПДн субъекту ПДн (например, регулирование оператором ПДн);

f) обработчик ПДн предоставляет ПДн оператору ПДн (например, после обслуживания/выполнения сервиса, для которого они были предназначены).

Роли субъекта ПДн, оператора ПДн, обработчика ПДн и третьей стороны в данных сценариях приведены в таблице 1.

Необходимо различать обработчиков ПДн и третью сторону, потому что при пересылке ПДн обработчику ПДн правовой контроль за ПДн остается функцией первоначального оператора ПДн, тогда как третья сторона оправданно может стать самостоятельным оператором ПДн после получения запрашиваемых ПДн. Например, когда третья сторона принимает решение о передаче ПДн, полученных от оператора ПДн, другой стороне, она будет действовать как оператор ПДн с ее собственными правами и поэтому больше не будет являться третьей стороной.

Можно идентифицировать следующие сценарии, формирующие потоки ПДн между операторами ПДн и обработчиками ПДн, с одной стороны, и третьей стороной, с другой стороны:

g) оператор ПДн предоставляет ПДн третьей стороне (например, в контексте делового соглашения);

h) обработчик ПДн предоставляет ПДн третьей стороне (например, по указанию оператора ПДн).

Роли оператора ПДн и третьей стороны в этих сценариях также показаны в таблице 1.

Таблица 1 — Возможные потоки ПДн между субъектом ПДн, оператором ПДн, обработчиком ПДн и третьими сторонами и их роли

Сценарий	Субъект ПДн	Оператор ПДн	Обработчик ПДн	Третья сторона
a)	Поставщик ПДн	Получатель ПДн	—	—
b)	—	Поставщик ПДн	Получатель ПДн	—
c)	Поставщик ПДн	—	Получатель ПДн	—
d)	Получатель ПДн	Поставщик ПДн	—	—
e)	Получатель ПДн	—	Поставщик ПДН	—
f)	—	Получатель ПДн	Поставщик ПДН	—
g)	—	Поставщик ПДн	—	Получатель ПДн
h)	—	—	Поставщик ПДн	Получатель ПДн

4.4 Распознавание персональных данных

Чтобы определить, считается ли физическое лицо идентифицируемым, должны быть приняты во внимание некоторые факторы. В частности, следует учитывать все средства, которые могут оправданно использоваться лицом, заинтересованным в обеспечении безопасности ПДн, хранящим данные, или любой другой стороной для идентификации этого физического лица. Информационные системы персональных данных должны поддерживать механизмы, информирующие субъекта ПДн о таких ПДн, и предоставлять физическому лицу соответствующие меры обеспечения безопасности ПДн при совместном использовании этой информации. В следующих подпунктах содержится дополнительное разъяснение того, как определить, следует ли рассматривать субъекта ПДн в качестве идентифицируемого.

4.4.1 Идентификаторы

В определенных случаях идентифицируемость субъекта ПДн может быть очевидной (например, когда информация содержит или связана с идентификатором, который используется для обращения или связи с субъектом ПДн). Информация может быть отнесена к ПДн в следующих случаях:

- если она содержит или связана с идентификатором, который относится к физическому лицу (например, номер социального страхования);
- если она содержит или связана с идентификатором, который может быть легко связан с физическим лицом (например, номер и серия паспорта, номер счета);
- если она содержит или связана с идентификатором, который может использоваться для установления связи с идентифицируемым физическим лицом (например, точное географическое местоположение, номер телефона);
- если она содержит ссылку, которая связывает данные с любым из идентификаторов, приведенных ранее.

4.4.2 Другие отличительные характеристики

Идентифицируемость является способностью определения физического лица, к которому относится данный набор ПДн. Поэтому информация не обязательно должна быть связана с идентификатором, чтобы считаться ПДн. Информацию можно считать ПДн, если она содержит или связана с характеристикой, которая отличает физическое лицо от других физических лиц (например, биометрические данные).

Любой атрибут, имеющий числовое, буквенное или буквенно-числовое значение и который уникально опознает субъекта ПДн, следует рассматривать как отличительную характеристику. Необходимо отметить, что независимо от того, отличает ли данная характеристика физическое лицо от других физических лиц, она может измениться от контекста использования. Например, фамилии физического лица может быть недостаточно, чтобы опознать его в глобальном масштабе, но будет достаточно, чтобы отличить физическое лицо в масштабе организации.

Кроме того, могут существовать ситуации, в которых физическое лицо является идентифицируемым, даже если не существует никакого единственного признака, который уникально определяет его или ее. В этом случае комбинация нескольких признаков, взятых вместе, отличает физическое лицо от других физических лиц. Возможность отнесения некоего физического лица к идентифицируемому, исходя из комбинации признаков, может также зависеть от конкретной области. Например, комбинации

признаков «женщина», «45», «адвокат» может быть достаточно для идентификации некоего физического лица в пределах определенной организации, но зачастую этих признаков бывает недостаточно для идентификации этого же физического лица за пределами этой же организации.

В таблице 2 приведены некоторые примеры атрибутов, которые могут являться ПДн в зависимости от сферы деятельности. Эти примеры являются информативными.

Таблица 2 — Примеры атрибутов, используемых для идентификации физических лиц

Примеры
Возраст или особые потребности уязвимых физических лиц; заявление о криминальном поведении; любая информация, собранная во время оказания медицинских услуг; номер банковского счета или кредитной карты; биометрический идентификатор; информация о кредитной карте; осуждение в уголовном порядке или совершенные преступления; отчеты об уголовном расследовании; абонентский номер; дата рождения; информация о диагностике состояния здоровья; нетрудоспособность; документ о нетрудоспособности; сведения о заработной плате служащих и файлы отдела кадров; финансовая информация; пол; данные GPS о местоположении; траектории GPS; домашний адрес; IP-адрес; информация о местоположении, полученная от телекоммуникационных систем; история болезни; фамилия; государственные идентификаторы, например, номер и серия паспорта; адрес личной электронной почты; личные идентификационные номера (PIN-коды) или пароли; личные интересы, полученные из отслеживания web-сайтов Интернет; личный или поведенческий стереотип; номер личного телефона; фотография или видео, по которым можно идентифицировать человека; предпочтения, касающиеся продуктов и услуг; расовое или этническое происхождение; религиозные или философские убеждения; сексуальная ориентация; членство в профсоюзах; счет за коммунальные услуги

4.4.3 Информация, которая связана или может быть связана с субъектом ПДн

Если рассматриваемая информация не идентифицирует субъекта ПДн, то должно быть определено, связана ли эта информация или может быть связана с идентификационными данными физического лица.

После установления связи с идентифицируемым физическим лицом необходимо решить, сообщает ли что-либо информация о данном физическом лице, например, информация может быть связана с его (или ее) характеристиками либо поведением. Примерами информации о физическом лице являются истории болезни, финансовая информация или личные интересы, полученные посредством отслеживания использования web-сайтов Интернет. Простые сообщения об отличительных чертах физического лица, таких как возраст или пол физического лица, могут также квалифицировать связанную с ним информацию как ПДн. Независимо от этого, если связь с идентифицируемым физическим лицом может быть установлена, такая информация также должна обрабатываться как ПДн.

4.4.4 Псевдонимные данные

Чтобы ограничить возможность операторов и обработчиков ПДн идентифицировать субъекта ПДн, идентификационная информация может быть заменена псевдонимами. Такая замена обычно выполняется поставщиком ПДн до передачи ПДн получателю ПДн, в частности, как указано в сценариях a), b), c), g), h) таблицы 1.

При некоторых процессах бизнеса полагаются на назначенных обработчиков, которые выполняют замену и контролируют таблицу или функцию назначения. Как правило, это бывает тогда, когда существует необходимость обработки чувствительных данных лицами, заинтересованными в обеспечении защиты ПДн, не производившими их сбор.

Замена идентификационной информации на псевдонимы обеспечивает следующее:

a) оставшиеся атрибуты, связанные с псевдонимами, недостаточны для идентификации субъекта ПДн, к которому они относятся;

b) псевдонимы назначаются так, чтобы их использование для выполнения обратного действия не могло осуществляться даже при затрачивании значительных усилий лицами, заинтересованными в обеспечении защиты ПДн, кроме тех лиц, которые уполномочены это делать.

Применение псевдонимов сохраняет возможность установления связи. Можно установить связь между различными данными, связанными с одним и тем же псевдонимом. Чем больше объем данных, связанных с определенным псевдонимом, тем больше риск того, что свойство будет нарушено. Более того, чем меньше группа физических лиц, к которым относится набор псевдонимных данных, тем больше вероятность того, что субъект ПДн станет идентифицируемым. Признаки, содержащиеся непосредственно в информации, о которой идет речь, и признаки, которые могут быть легко связаны с этой информацией (например, посредством использования поисковой системы или перекрестных ссылок с другими базами данных), должны быть приняты во внимание при определении того, относится или не относится информация к идентифицируемому физическому лицу.

Применение псевдонимов является действием, в определенном смысле противоположным обезличиванию. Процессы обезличивания также обеспечивают свойства a) и b), приведенные ранее, но нарушают возможность установления связи. Во время обезличивания идентификационная информация либо удаляется, либо заменяется псевдонимами, для которых функция или таблица назначения уничтожаются. Поэтому обезличенные данные больше не являются ПДн.

4.4.5 Метаданные

ПДн могут храниться в информационной системе персональных данных таким образом, что они не будут являться видимыми для пользователя системы (т. е. субъекта ПДн). Примерами такой информации являются фамилия субъекта ПДн, хранящаяся как метаданные в свойствах документа, комментарии или отслеженные изменения, хранящиеся как метаданные в документе по подготовке текстов. Если субъекту ПДн станет известно о существовании ПДн или обработке ПДн для этой цели, то он, возможно, предпочтет, чтобы ПДн не обрабатывались таким образом или не использовались совместно.

4.4.6 Незапрашиваемые персональные данные

ПДн, которые не были запрошены оператором ПДн или обработчиком ПДн (т. е. получены непреднамеренно), могут также храниться в информационной системе персональных данных. Например, субъект ПДн потенциально мог бы предоставить ПДн оператору ПДн, которые последний не запрашивал или не отыскивал (например, дополнительные ПДн, предоставляемые в контексте в форме анонимной обратной связи на web-сайте). Риск сбора незапрашиваемых ПДн может быть уменьшен путем рассмотрения мер защиты ПДн во время проектирования системы (также известных как понятие «обеспечение защиты ПДн через проектирование»).

4.4.7 Чувствительные персональные данные (специальные категории ПДн)

Чувствительность распространяется на все ПДн, из которых могут быть получены специальные категории ПДн. Например, медицинские предписания могут предоставить подробную информацию о здоровье субъекта ПДн. Даже если ПДн не содержат прямую информацию о сексуальной ориентации или здоровье субъекта ПДн, но могут быть использованы для получения подобной информации, то такие ПДн могут являться чувствительной информацией. Для целей настоящего стандарта ПДн следует рассматривать как чувствительную информацию там, где это возможно.

В некоторых странах понятие чувствительных ПДн явно определено в законе. Примером является информация о расовой принадлежности, этническом происхождении, религиозных или философских убеждениях, политических взглядах, членстве в профсоюзах, сексуальной жизни или ориентации, а также о физическом или психическом здоровье субъекта ПДн. В других странах чувствительные ПДн могут включать в себя информацию, которая могла бы способствовать «краже личности» (идентифика-

ционных данных) или иным образом приводить к значительному финансовому ущербу для физического лица (например, номера кредитных карт, информация о банковском счете или государственные идентификаторы, такие как номер и серия паспорта, номера страховых свидетельств, номера водительских удостоверений), и информацию, которая могла бы использоваться для определения местонахождения субъекта ПДн в реальном масштабе времени.

Обработка чувствительных ПДн требует применения специальных мер. Во многих странах обработка чувствительных ПДн может быть запрещена действующим законом, даже если субъект ПДн дал согласие на их обработку. Некоторые страны могут потребовать выполнения определенных мер обеспечения безопасности при обработке определенных типов чувствительных ПДн (например, требование зашифровать медицинские ПДн при передаче их по общедоступной сети).

4.5 Требования к мерам обеспечения безопасности персональных данных

Организации заинтересованы в обеспечении безопасности ПДн по разным причинам: чтобы защищать право на обеспечение безопасности ПДн субъекта, соответствовать правовым и нормативным требованиям, выполнять обязанности корпорации, повышать доверие клиентов и т. д. Цель данного подраздела заключается в определении различных факторов, которые могут влиять на требования к мерам защиты ПДн, являющиеся соответствующими для отдельных организаций или лиц, обрабатывающих ПДн и заинтересованных в обеспечении права на защиту ПДн.

Требования к мерам защиты ПДн могут затрагивать различные аспекты обработки ПДн, например сбор и сохранение ПДн, передачу ПДн третьим сторонам, договорные взаимоотношения между операторами ПДн, обработчиками ПДн, трансграничную передачу ПДн и т. д. Требования к мерам защиты ПДн могут также различаться по специфике. Они могут быть общими по характеру, например состоять из определенного количества высокоуровневых принципов защиты ПДн, которые, как ожидается, организация будет принимать во внимание при обработке ПДн. Однако требования к мерам защиты ПДн могут включать к себя очень специфические ограничения на обработку определенных типов ПДн или предписывать реализацию специфических мер обеспечения безопасности ПДн.

Разработке какой-либо системы ИКТ, осуществляющей обработку ПДн, должна предшествовать идентификация соответствующих требований к мерам защиты ПДн. Последствия обеспечения защиты ПДн, связанные с новыми или значительно модифицированными системами, участвующими в обработке ПДн, должны быть приняты во внимание (разрешены) до того, как такие информационные системы персональных данных будут реализованы. В плановом порядке организации выполняют широкий спектр деятельностей по управлению рисками и разрабатывают профили риска, относящиеся к их информационным системам персональных данных.

Управление рисками определяется как «скоординированные действия по руководству и управлению организацией в отношении риска» (ISO Guide 73:2009). Процесс управления рисками защиты ПДн включает в себя следующие процессы:

- установление контекста путем осмысления организации (например, обработка ПДн, обязанности), технической среды и факторов, влияющих на управление рисками нарушения безопасности ПДн (т. е. правовые и нормативные факторы, договорные факторы, факторы бизнеса и другие факторы);
- оценку риска путем идентификации, анализа и оценивания рисков для субъектов ПДн (риски, которые могут повлиять на них неблагоприятным образом);
- обработку риска путем определения требований по защите ПДн, идентификации и реализации мер обеспечения безопасности ПДн для предотвращения или уменьшения рисков для субъектов ПДн;
- коммуникации и консультирование путем получения информации от заинтересованных сторон, достижения согласия по каждому процессу управления рисками, а также информирования субъектов ПДн и сообщения им о рисках и мерах обеспечения безопасности ПДн;
- мониторинг и пересмотр путем отслеживания рисков, мер обеспечения безопасности ПДн, а также усовершенствования процесса.

Одним из результатов может быть оценка влияния защиты ПДн, которая является составной частью управления рисками, направленного на обеспечение соблюдения законодательных требований в части защиты ПДн, и оценка последствий обеспечения защиты ПДн в новых или существенно измененных программах или видах деятельности. Оценки влияния защиты ПДн должны быть оформлены в рамках более широкой структуры управления рисками организации.

Рисунок 1 — Факторы, влияющие на управление рисками в области защиты ПДн

Требования к мерам защиты ПДн идентифицируются как часть общего процесса управления рисками обеспечения прав субъектов ПДн, на который оказывают влияние следующие факторы (как показано на рисунке 1 и описано далее):

- правовые и нормативные факторы, направленные на защиту прав физического лица и защиту его ПДн;

- договорные факторы, такие как соглашения между несколькими различными субъектами, политики организации и обязательные корпоративные правила (Изменение Amd.1:2018);

- факторы бизнеса, предопределенные специфичными бизнес-приложениями или, в отдельных случаях, специфичным контекстом;

- другие факторы, которые могут влиять на проектирование информационной системы персональных данных и связанные с ними требования к мерам обеспечения безопасности ПДн.

4.5.1 Правовые и нормативные факторы

Требования к мерам обеспечения безопасности ПДн часто отражены в (1) международных, национальных и местных законах, (2) постановлениях, (3) судебных решениях или (4) договорных соглашениях с советами трудовых коллективов или другими организациями работников. Некоторые примеры местного и национального законодательства включают в себя законы о защите данных, о защите прав потребителя, законы о предупреждении нарушений, законы о хранении данных и трудовое законодательство. Соответствующие международные законы могут включать в себя правила, затрагивающие трансграничную передачу ПДн. Операторы ПДн должны быть осведомлены обо всех соответствующих требованиях к мерам обеспечения безопасности ПДн, вытекающих из правовых или нормативных факторов. Для достижения этой цели операторы могут действовать в тесном сотрудничестве с юрисконсультами. В то время как для многих стран ответственность за соблюдение требований, в конечном счете, несет оператор ПДн, все стороны, участвующие в обработке ПДн, также должны занять активную позицию в определении соответствующих требований обеспечения защиты ПДн, вытекающих из правовых и нормативных факторов.

4.5.2 Договорные факторы

Договорные обязательства также могут влиять на требования к мерам защиты ПДн. Эти обязательства могут являться результатом соглашений между несколькими субъектами и соглашений с отдельными субъектами, например соглашения обработчиков ПДн, соглашения операторов ПДн и третьих сторон. Например, лицо, заинтересованное в обеспечении защиты ПДн, может потребовать, чтобы третьи стороны использовали определенные меры обеспечения безопасности ПДн и согласовывали требования о распоряжении специфическими ПДн до передачи им ПДн. Требования к мерам защиты ПДн могут также определяться политикой организации и обязательными корпоративными правилами, которые лицо, заинтересованное в обеспечении защиты ПДн, определило само для себя, например для защиты торговой марки от утраты репутации в случае нарушения прав субъектов на обеспечение безопасности своих ПДн.

В принципе любая сторона, имеющая доступ к ПДн, должна быть поставлена в известность о своих обязательствах со стороны оператора(ов) ПДн в формализованном виде, например путем заключения договора с третьей стороной. Такие соглашения, вероятно, будут содержать ряд требований к мерам защиты ПДн, которые получатели ПДн должны принимать во внимание. В некоторых странах национальные и региональные органы могут иметь установленные правовые и договорные инструменты, делающие возможной передачу ПДн третьим сторонам (Изменение Amd.1:2018).

4.5.3 Факторы бизнеса

На требования к мерам обеспечения безопасности ПДн могут также влиять факторы бизнеса, к которым относятся определенные характеристики, предусмотренные для применения, или контекст их использования. Факторы бизнеса могут широко варьироваться в зависимости от типа лица, заинтересованного в обеспечении защиты ПДн, и вида бизнеса. Например, они могут иметь отношение к сегменту, в котором организация функционирует (например, отраслевые нормы, кодекс поведения, лучшие практики, стандарты), или к характеру модели бизнеса (например, онлайновые сервисы в непрерывном режиме, сервисы совместного использования информации, банковские приложения).

Многие бизнес-факторы не оказывают прямого влияния на требования к защите конфиденциальности. Предполагаемое использование ПДн, вероятно, повлияет на реализацию организацией политики конфиденциальности, а также на выбор мер обеспечения безопасности ПДн. Однако организация не должна изменять принципы защиты ПДн, на которые она подписывается из-за этого. Например, для предоставления определенной услуги может потребоваться поставщик услуг, который может собирать дополнительные ПДн для того, чтобы больше сотрудников обрабатывало отдельные виды ПДн. Тем не менее, надзорному органу идентификационных данных (ПДн), который поддерживает принципы, содержащиеся в правилах обращения с ПДн, следует тщательно оценить, какие типы ПДн необходимы для предоставления услуги (принцип ограничения сбора), и ограничить обработку ПДн сотрудниками организации, предоставляющей услуги, до уровня, необходимого для того, чтобы выполнять свои обязанности (принцип минимизации данных) (Изменение Amd.1:2018).

4.5.4 Другие факторы

Наиболее важный фактор, который следует учитывать организации при идентификации требований к мерам обеспечения безопасности ПДн, связан с предпочтениями субъектов ПДн в сфере защиты ПДн. Персональная позиция физического лица по отношению к защите ПДн и то, что оно вкладывает в понятие «риски», может зависеть от ряда факторов, включающих: понимание физическим лицом используемой технологии, их происхождение, предоставляемую информацию, назначение транзакций, приобретенный опыт, а также социально-психологические факторы.

Проектировщики информационной системы персональных данных должны понимать вероятные проблемы обеспечения защиты ПДн субъектов ПДн и типы ПДн, которые будут обрабатываться с помощью этой системы. Проектировщики, так же как разработчик системы или приложения или поставщик услуг, изучают целевую аудиторию клиентов, нуждающихся в обеспечении защиты ПДн, для того чтобы понять их ожидания и предпочтения относительно обеспечения защиты ПДн. Проектировщики информационных систем персональных данных не всегда могут предоставить субъекту ПДн выбор, который бы соответствовал их предпочтению по обеспечению защиты ПДн.

Примеры предпочтений по обеспечению защиты ПДн могут включать в себя предпочтение анонимности или назначения псевдонимов, возможность ограничения доступа к конкретным ПДн или возможность ограничения цели обработки ПДн. До определенной степени субъекту ПДн предоставляется выбор предпочтения обработки его данных, например использовать ли ПДн во вторичных целях, таких как маркетинг. Способность выразить предпочтения, не влияющие неблагоприятным образом на защиту ПДн, могут быть реализованы с помощью графического интерфейса пользователя информационной системы персональных данных. Это может помочь субъекту ПДн сделать выбор, представив набор предопределенных вариантов общих предпочтений в части обеспечения защиты ПДн с использованием легко понимаемого языка. Реализация пользовательского интерфейса может быть основана на таких элементах, как поля выбора и выпадающее меню.

В дополнение к факторам, перечисленным в предыдущих пунктах, существуют другие факторы, которые могут влиять на проектирование информационных систем персональных данных и связанные с ними требования к мерам обеспечения безопасности ПДн. Например, на требования к мерам обеспечения безопасности ПДн могут влиять системы внутреннего контроля или технические стандарты, принятые организацией (например, такой рекомендуемый стандарт, как стандарт ISO).

4.6 Политики защиты персональных данных

Высшее руководство организации, участвующее в обработке ПДн, призвано создать политику защиты ПДн. Политика защиты ПДн должна:

- соответствовать назначению организации;
- предоставлять структуру для установления целей;
- включать обязательство соответствовать применимым требованиям к мерам обеспечения безопасности ПДн;
- включать обязательство в части непрерывного совершенствования;
- быть озвучена в пределах организации;
- быть доступной заинтересованным сторонам.

Организация должна оформлять свою политику защиты ПДн в письменной форме. Если организация, обрабатывающая ПДн, является обработчиком ПДн, то эти политики могут в значительной степени определяться оператором ПДн. Политика защиты ПДн должна быть дополнена более детализированными правилами и обязательствами различных лиц, заинтересованных в защите ПДн, участвующих в обработке ПДн (например, процедуры для конкретных ведомств или сотрудников). Кроме того, меры обеспечения безопасности, которые используются для проведения в жизнь политики защиты ПДн в конкретных условиях (например, контроль доступа, обеспечение уведомлений, аудиты и т. д.), должны быть документированы четким образом.

Термин «политика защиты ПДн» часто используется для упоминания как о внутренних, так и о внешних политиках защиты ПДн. Внутренняя политика защиты ПДн документирует цели, правила, обязательства, ограничения и (или) формирование мер обеспечения безопасности ПДн, которые адаптированы организацией к удовлетворению требований к мерам обеспечения безопасности ПДн, являющихся важными для обработки ПДн. Внешние политики защиты ПДн предоставляются внешним поставщикам организации с уведомлениями о практиках организации защиты ПДн, а также о другой важной информации, например идентификационные данные и официальный адрес оператора ПДн, точки контакта, откуда субъекты ПДн могли бы получать дополнительную информацию, и т. д. В контексте такой структуры термин «политика защиты ПДн» используется для ссылки на внутреннюю политику защиты ПДн организации. На внешнюю политику защиты ПДн ссылаются как на уведомления.

4.7 Меры обеспечения безопасности персональных данных

Организации должны идентифицировать и реализовывать меры обеспечения безопасности ПДн, чтобы соответствовать требованиям к мерам обеспечения безопасности ПДн, определенным оценкой риска нарушения безопасности ПДн и процессом обработки. Кроме того, реализуемые меры обеспечения безопасности ПДн должны быть документально оформлены, как часть документации по оценке риска обеспечения безопасности ПДн организации. Определенные виды обработки ПДн, возможно, потребуют применения специальных мер обеспечения безопасности ПДн, потребность в которых станет очевидной, как только намеченные действия будут тщательно проанализированы. Оценка риска может оказать помощь организациям в идентификации специфических рисков нарушения безопасности ПДн для рассматриваемых видов обработки.

Организация должна приложить усилия, чтобы разработать собственные меры обеспечения безопасности ПДн, как часть общего подхода «обеспечения защиты ПДн через проектирование», т. е. обеспечение безопасности ПДн должно приниматься в расчет на стадии проектирования систем, обрабатывающих ПДн, а не сдвигаться на последующие этапы.

Поскольку затрагиваются меры обеспечения информационной безопасности, важно отметить, что не вся обработка ПДн требует одного и того же уровня или типа защиты. Организации должны различать операции по обработке ПДн в соответствии с их специфическими рисками, чтобы помочь определению того, какие меры обеспечения информационной безопасности и в каких случаях являются соответствующими. Управление рисками может рассматриваться как основной метод этого процесса, а идентификация мер обеспечения безопасности ПДн также должна являться неотъемлемой частью структуры управления информационной безопасностью организации.

5 Принципы защиты персональных данных

5.1 Общий обзор принципов защиты персональных данных

Принципы конфиденциальности, описанные в настоящем стандарте, основаны на существующих принципах, разработанных рядом стран и международных организаций. Эти правила нацелены на внедрение принципов защиты ПДн в информационных системах персональных данных и развитие систем управления защитой данных, которые должны быть внедрены в рамках информационных систем организации. Принципы защиты ПДн должны использоваться при проектировании, разработке и внедрении политики конфиденциальности и мер обеспечения безопасности ПДн. Кроме того, они могут быть использованы в качестве основы при мониторинге и измерении эффективности, анализе и внедрении лучших практик, проведении аудита аспектов программы управления конфиденциальностью в организации (Изменение Amd.1:2018).

Несмотря на различия в социальных, культурных, правовых и экономических факторах, которые могут ограничивать применение этих принципов в одном и том же контексте, рекомендуется применение любых принципов, приведенных в настоящем стандарте. Любые исключения из этих принципов должны быть ограничены.

Основу настоящего стандарта формируют принципы обеспечения безопасности ПДн, которые приведены в таблице 3.

Таблица 3 — Принципы обеспечения безопасности ПДн

Принципы обеспечения безопасности ПДн
1 Согласие и выбор
2 Законность цели и ее спецификация
3 Ограничение на сбор информации
4 Минимизация данных
5 Ограничения в отношении использования, хранения и раскрытия
6 Точность и качество
7 Открытость, прозрачность и уведомление
8 Индивидуальное участие и доступ
9 Ответственность
10 Информационная безопасность
11 Соответствие безопасности ПДн

5.2 Согласие и выбор

Соблюдение принципа согласия означает:

- предоставление субъекту ПДн выбора между разрешением или недопущением обработки его ПДн, за исключением случаев, когда субъект ПДн не может прямо дать согласие или когда соответствующий закон разрешает проведение обработки ПДн без согласия физического лица. Выбор субъектом ПДн должен быть свободным и основан на знаниях;
- получение согласия на обработку от субъекта ПДн для сбора или иной обработки специальных категорий ПДн, за исключением случаев, когда соответствующий закон разрешает обработку специальных категорий ПДн без согласия физического лица;
- информирование субъекта ПДн (до получения его согласия) о его правах в соответствии с принципом индивидуального участия и доступа;
- предоставление субъекту ПДн (до получения его согласия) информации, обозначенной принципами открытости, прозрачности и уведомления;
- объяснение субъекту ПДн последствий получения согласия на предоставление и обработку ПДн или отказа от согласия.

Необходимо предоставить субъекту ПДн возможность выбора того, каким образом его ПДн будут обрабатываться, и разрешить ему отозвать согласие без затруднений и бесплатно. Реализация запроса должна выполняться в соответствии с законодательством по обеспечению безопасности ПДн. Даже если согласие будет отозвано, оператор ПДн может сохранить некоторые ПДн на определенный период времени в порядке исполнения правовых или договорных обязательств (например, реализация требований законодательства по хранению данных или по обязательной отчетности). В случае, когда обработка ПДн базируется не на согласии, а на другой правовой основе, оператор ПДн должен быть уведомлен об этом. В тех случаях, когда субъект ПДн имеет возможность отзыва согласия, но не решается так поступить, эти ПДн должны быть защищены от обработки для какой-либо незаконной цели.

Для оператора ПДн соблюдение принципа выбора означает:

- предоставление субъекту ПДн четких, известных, доступных, легко понимаемых, по умеренной стоимости механизмов для осуществления выбора и предоставления согласия в отношении обработки его ПДн во время сбора, первоначального использования или после, когда это будет целесообразно;
- осуществление предпочтений субъекта ПДн, которые выражены в его согласии.

Кроме того, соответствующий закон может определить дополнительные условия в отношении согласия и другие основания для обработки ПДн, отличные от согласия (например, выполнение условий контракта, жизненные интересы субъекта ПДн или соблюдение закона). Применимый закон в некоторых случаях предусматривает, что согласие субъекта ПДн не является достаточным юридическим основанием для обработки ПДн (например, согласие подростка, данное без одобрения родителей или опекуна). Кроме того, следует учитывать дополнительные требования при передаче ПДн между различными государствами. Оператор ПДн несет ответственность за соблюдение этих дополнительных требований до обработки и передачи данных.

5.3 Законность цели и ее описание

Соблюдение принципа законности цели и ее описания означает:

- обеспечение уверенности в том, что цели исполняются в соответствии с законом и основываются на других правовых обязательствах;
- информирование субъекта ПДн о цели(ях) в период, предшествующий сбору информации или ее использованию впервые для реализации новой цели;
- использование для описания цели таких формулировок, которые четко и соответствующим образом адаптированы к специфике реализации цели;
- разъяснение необходимости обработки специальных категорий ПДн, если существует потребность в таком разъяснении.

В отношении чувствительных ПДн могут применяться более строгие правила, касающиеся цели обработки. Для соблюдения законности цели может потребоваться правовое основание или специальное разрешение службы защиты данных или правительственных структур. Обработка не должна осуществляться, если цели обработки ПДн не соответствуют действующему законодательству.

5.4 Ограничение на сбор

Соблюдение принципа ограничения на сбор означает:

- ограничение сбора ПДн до такой степени, которая определяется рамками применяемого закона и строго необходимой(ыми) целью(ями).

Организации не должны собирать личную информацию хаотично. Количество и тип собранной информации должны быть ограничены до такой степени, которая является необходимой для осуществления (в рамках закона) реализации цели(ей), точно определенной(ых) оператором ПДн. Организации, прежде чем приступить к сбору ПДн, должны тщательно рассмотреть те ПДн, которые могут быть затребованы для осуществления особой цели. Организации должны документировать типы накопленных ПДн, а также правомерность их накопления для выполнения деятельности, являющейся частью их политик и практик по обработке информации.

Оператор ПДн может выразить желание собирать дополнительные ПДн с иной целью, чем предоставление конкретной услуги, требуемой субъекту ПДн (например, в целях прямого маркетинга). В зависимости от полномочий такая дополнительная информация может быть собрана только при согласии субъекта ПДн. Возможно также, что сбор определенной информации будет разрешен с помощью соответствующего закона. Когда это допустимо, субъекту ПДн должна быть дана возможность выбора: предоставлять или не предоставлять такую информацию. Субъект ПДн также должен быть четко осве-

домлен о том обстоятельстве, что его ответные действия на такие запросы о дополнительной информации не являются обязательными.

5.5 Минимизация данных

Минимизация данных тесно связана с принципом «ограничение на сбор», но является более широким понятием. В то время как «ограничение на сбор» связано со сбором ограниченных данных по отношению к указанной цели, минимизация данных строго минимизирует обработку ПДн.

Соблюдение принципа минимизации данных означает разработку и реализацию процедур по обработке данных и систем такими способами, чтобы:

- минимизировать персональные данные, которые обрабатываются, а также количество заинтересованных в обеспечении конфиденциальности сторон и лиц, чьи ПДн подлежат разглашению или которым разрешено их обрабатывать;
- обеспечить принятие принципа «необходимости знать» (т. е. разрешение обрабатывать только те ПДн, которые необходимы для выполнения своих служебных обязанностей в рамках законной цели обработки ПДн);
- использовать или предлагать в качестве вариантов по умолчанию, где это возможно, взаимодействия и транзакции, которые не вовлекают в процесс идентификации субъектов ПДн, снижают наблюдаемость их поведения и ограничивают привлекательность собранных ПДн;
- безопасно уничтожать ПДн, когда это возможно на практике, в частности, в случае истечения срока обработки ПДн и отсутствия законных требований к их хранению (Изменение Amd.1:2018).

5.6 Ограничения в отношении использования, хранения и раскрытия

Соблюдение принципа ограничения в отношении использования, хранения и раскрытия означает:
- ограничение использования, хранения и раскрытия (включая передачу) ПДн, которые необходимы, чтобы выполнять специфические, определенные и законные цели;
- ограничение использования ПДн для целей, определенных оператором ПДн до сбора информации, за исключением особой цели, прямо определенной законом;
- хранение ПДн в течение такого промежутка времени, который необходим для выполнения заявленных целей, и последующее безопасное уничтожение или обезличивание ПДн;
- блокирование (то есть архивирование, обеспечение безопасности и исключение дальнейшей обработки) любых ПДн, когда заявленные цели достигнуты, но применимый закон требует обеспечения хранения.

Когда осуществляется трансграничная передача ПДн, оператор ПДн должен быть осведомлен обо всех дополнительных международных или региональных требованиях, специфичных для международных пересылок.

5.7 Точность и качество

Соблюдение принципа точности и качества означает:
- обеспечение уверенности в том, что обрабатываемые ПДн являются правильными, полными, обновляемыми (за исключением случаев, когда имеется законное основание для хранения данных, утративших свою актуальность), адекватными и значимыми для цели использования;
- обеспечение уверенности в достоверности ПДн, полученных от источника, не являющегося субъектом ПДн, до их обработки;
- подтверждение соответствующими способами юридической силы и корректности претензий от субъекта ПДн до выполнения любых изменений в ПДн (чтобы обеспечить уверенность в том, что изменения санкционированы должным образом) там, где это необходимо выполнить;
- установление процедур сбора ПДн в целях обеспечения точности и качества;
- установление механизмов управления, обеспечивающих периодическую проверку точности и качества собранных и сохраненных ПДн.

Этот принцип особенно важен в тех случаях, когда данные могут использоваться для предоставления или отказа в праве на получение материальной выгоды для физического лица или когда неточные данные при других обстоятельствах могут привести к существенному ущербу для физического лица.

5.8 Открытость, прозрачность и уведомление

Соблюдение принципа открытости, прозрачности и уведомления означает:

- предоставление субъекту ПДн четкой и легкодоступной информации о политиках, процедурах и практических приемах операторов ПДн, относящихся к обработке ПДн;
- включение в уведомления факта обработки ПДн; цели, для которой осуществляется обработка; типов лиц, заинтересованных в защите ПДн, которым могут быть раскрыты ПДн, и идентификационных данных оператора ПДн, включая контактную информацию оператора ПДн;
- раскрытие вариантов выбора и средств, предлагаемых оператором ПДн, субъекту ПДн для целей ограничения использования информации, а также для доступа, корректировки и пересылки его информации;
- уведомление субъектов ПДн о существенных изменениях в процедурах, выполняемых при обращении с ПДн.

Может потребоваться обеспечение прозрачности общей информации, логически лежащей в основе обработки ПДн, особенно если от результатов обработки зависит решение, влияющее на субъекта ПДн. Лица, заинтересованные в обеспечении безопасности ПДн, участвующие в обработке ПДн, должны владеть определенной информацией о своих политиках и практиках, относящихся к управлению защитой ПДн, которая легко доступна для общественного пользования. Все договорные обязательства, которые влияют на обработку ПДн, должны быть документированы и утверждены в организации соответствующим образом. О них должно быть также известно за пределами организации до той степени, когда эти обязательства не будут являться конфиденциальными.

Кроме того, цель обработки ПДн должна быть достаточно детализирована, чтобы дать возможность субъекту ПДн понять:

- определенные ПДн, требующиеся для конкретной цели;
- определенную цель для сбора ПДн;
- определенную обработку (включая механизмы сбора, передачи и хранения);
- типы уполномоченных физических лиц, кто будет осуществлять доступ к ПДн и кому ПДн могут передаваться;
- указанные требования к хранению и утилизации ПДн (Изменение Amd.1:2018).

5.9 Индивидуальное участие и доступ

Соблюдение принципа индивидуального участия и доступа означает:

- предоставление субъектом ПДн возможности доступа к ПДн и возможности проверки их ПДн при условии, что их идентификационные данные сначала аутентифицируются с соответствующим уровнем обеспечения уверенности и такой доступ не запрещен действующим законом;
- наличие у субъектов ПДн возможности оспорить точность и полноту ПДн и добиться внесения в них поправок, исправлений или их удаления;
- предоставление возможности любых изменений или удалений обработчикам ПДн и третьим лицам, которым ПДн были раскрыты и где они стали известны (Изменение Amd.1:2018);
- установление процедур, позволяющих субъектам ПДн осуществить эти права простым, быстрым и эффективным способом, который не влечет за собой неуместное промедление или неоправданные затраты.

Оператор ПДн должен применять соответствующие меры защиты ПДн для обеспечения уверенности в том, что субъектам ПДн доступны строго их собственные ПДн, а не те, которые доступны другим субъектам ПДн, за исключением случаев, когда физическое лицо, осуществляющее доступ, действует в рамках полномочий от лица субъекта ПДн, который неспособен осуществлять свои права доступа. Применимый закон может предоставить физическому лицу право доступа, просмотра и, в определенных случаях, отказа от обработки ПДн. Если физическое лицо не удовлетворено решением проблемы, то содержание неразрешенной проблемы должно быть зарегистрировано организацией. При необходимости, о существовании неразрешенной проблемы должны быть оповещены третьи стороны, имеющие доступ к рассматриваемой информации.

5.10 Ответственность

Обработка ПДн влечет за собой обязанность соблюдения осторожности и применения конкретных и целесообразных мер обеспечения безопасности ПДн. Соблюдение принципа ответственности означает:

- документирование и сообщение обо всех политиках, процедурах и методах обеспечения безопасности ПДн;
- назначение в пределах организации конкретного лица (которое может, в свою очередь, передать полномочия другим) ответственным за осуществление процедур и методов, связанных с политикой обеспечения безопасности ПДн;
- при передаче ПДн третьим сторонам обеспечение уверенности в том, что получатель третьей стороны будет обязан обеспечивать равноценный уровень безопасности ПДн через договорные или другие средства, такие как обязательные внутренние политики (соответствующий закон может содержать дополнительные требования, касающиеся передачи данных в международных масштабах);
- обеспечение соответствующего обучения сотрудников оператора ПДн, которым будет предоставляться доступ к ПДн;
- установление эффективных внутренних процедур обработки претензий и возмещения ущерба для их применения субъектами ПДн;
- информирование субъектов ПДн о нарушениях безопасности ПДн, которые могут нанести им существенный ущерб (если это не запрещено, например, при работе, связанной с применением закона), а также о мерах, принятых для устранения этих нарушений;
- уведомление всех лиц, заинтересованных в обеспечении безопасности ПДн, о нарушениях безопасности ПДн, как это требуется в некоторых странах (например, службами обеспечения безопасности данных) и в зависимости от уровня риска;
- доступ пострадавшему субъекту ПДн к соответствующим и эффективным санкциям и (или) механизмам, таким как исправление, исключение или восстановление, если произошло нарушение безопасности ПДн;
- рассмотрение процедур для компенсаций в ситуациях, в которых будет трудно или невозможно вернуть первоначальный статус ПДн физического лица в исходное состояние.

Меры, принимаемые для устранения нарушения безопасности, должны быть пропорциональны рискам, связанным с нарушением, но их реализация должна быть неотложной (за исключением ситуаций, когда это запрещено, например в процессе расследования правонарушения).

Создание процедур возмещения ущерба является важной частью установления ответственности. Возмещение ущерба предоставляет субъекту ПДн возможность сохранения ответственности оператора ПДн за ненадлежащее использование ПДн. Реституция — это форма возмещения, которая предполагает компенсацию пострадавшему субъекту ПДн. Это важно не только в случае кражи идентификационной информации («кражи личности»), вреда репутации или ненадлежащего использования ПДн, но также и в случае ошибок в модификации или изменении соответствующих ПДн.

В случае наличия процессов возмещения ущерба субъекты ПДн более уверенно идут на соглашение, так как принятый риск для физического лица в отношении результата в этом случае снижен. В отношении некоторых услуг возмещение легче определить (например, при финансовой потере), чем для других (например, кража идентификационной информации, ущерб для имиджа или репутации физического лица), в которых трудно оценить размер ущерба и предоставить компенсацию. Возмещение ущерба осуществляется лучше всего, когда оно основано на прозрачности и честности. Необходимые виды мер по возмещению ущерба могут регулироваться законом.

5.11 Информационная безопасность

Соблюдение принципа обеспечения информационной безопасности означает:

- защиту ПДн в рамках своих полномочий с помощью соответствующих мер обеспечения безопасности на эксплуатационном, функциональном и стратегическом уровне для обеспечения их целостности, конфиденциальности и доступности, а также защиту от рисков, таких как несанкционированный доступ, разрушение, использование, модификация или раскрытие либо потеря в течение всего их жизненного цикла;
- выбор обработчиков ПДн, которые предоставляют достаточные гарантии относительно как организационных, физических и технических мер обеспечения безопасности обработки ПДн, так и обеспечения соответствия этим мерам;

- базирование мер обеспечения безопасности ПДн на требованиях соответствующего законодательства, стандартов безопасности, а также результатах систематических оценок рисков безопасности, как описано в ISO 31000, и результатах анализа «затраты/выгода»;

- реализацию мер обеспечения безопасности соразмерно вероятности и серьезности потенциальных последствий, чувствительности ПДн, числу субъектов ПДн, которые могут быть затронуты, и контексту, в котором она производится;

- ограничение доступа к ПДн для пользователей, кроме тех лиц, кому такой доступ требуется для выполнения своих обязанностей, и ограничение доступа лицам, имеющим доступ к ПДн, только к той части ПДн, которые им необходимы для выполнения своих обязанностей;

- принятие решений относительно рисков и уязвимостей, обнаруженных с помощью оценок риска обеспечения защиты ПДн и процессов аудита;

- периодический пересмотр и переоценка мер обеспечения безопасности ПДн в процессе постоянного управления рисками безопасности.

5.12 Соответствие обеспечения безопасности персональных данных

Соблюдение принципа соответствия обеспечения безопасности ПДн означает:

- проверку и демонстрирование того, что обработка удовлетворяет требованиям защиты ПДн путем периодического проведения аудитов с использованием внутренних аудиторов или аудиторов доверенной третьей стороны;

- применение соответствующих внутренних мер обеспечения безопасности ПДн и механизмов независимого наблюдения, которые обеспечивают уверенность в соответствии применимому закону о защите ПДн, политикам и процедурам обеспечения безопасности ПДн;

- разработку и поддержку оценок риска нарушения безопасности ПДн для оценивания того, соответствуют ли инициативы по поставке программы или сервиса, включающие обработку ПДн, требованиям обеспечения безопасности ПДн.

Применимый закон может требовать, чтобы один или несколько наблюдательных органов были ответственными за мониторинг соответствия действующему закону о защите данных. В этих случаях поддержание принципа соответствия обеспечения безопасности ПДн также означает сотрудничество с наблюдательными органами и соблюдение их руководящих принципов и требований.

Приложение А
(справочное)

Соответствие между понятиями по ISO/IEC 29100 и понятиями по ISO/IEC 27000

Для упрощения использования серии стандартов ISO/IEC 27000 в специфическом контексте обеспечения защиты ПДн и интеграции понятий обеспечения безопасности ПДн в контексте ISO/IEC 27000 в таблице А.1 представлены взаимосвязи между понятиями по ISO/IEC 29100 и понятиями по ISO/IEC 27000.

Таблица А.1 — Соответствие между понятиями по ISO/IEC 29100 и понятиями по ISO/IEC 27000

Понятия по ISO/IEC 29100	Соответствие понятий по ISO/IEC 27000
Лицо, заинтересованное в обеспечении защиты ПДн	Причастная сторона
Персональные данные	Информационный актив
Нарушение безопасности ПДн	Инцидент информационной безопасности
Меры обеспечения безопасности ПДн	Меры обеспечения безопасности
Риск нарушения безопасности ПДн	Риск
Управление рисками нарушения безопасности ПДн	Менеджмент риска
Требования к мерам обеспечения безопасности ПДн	Цели применения мер обеспечения безопасности

Библиография

[1] ISO Guide 73, Risk management — Vocabulary

[2] ISO 31000, Risk management — Principles and guidelines

[3] ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD2) — Official Privacy Documents References, available at http://www.jtc1sc27.din.de

УДК 006.34:004.056:004.056.5:004.056.53:006.354 МКС 35.030

Ключевые слова: персональные данные (ПДн), оператор ПДн, субъект ПДн, принципы защиты ПДн, управление рисками

Технический редактор *И.Е. Черепкова*
Корректор *О.В. Лазарева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 05.07.2021. Подписано в печать 14.07.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,95.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru