2.8. Стандарты по защите персональных данных

В последние три года в Российской Федерации принято три национальных стандарта в области защиты персональных данных:

ГОСТ Р ИСО/МЭК 27018-2020 «Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки» введен в действие 1.06.2021 г. Он идентичен международному стандарту ISO/IEC 27018:2019 «Information technology — Security techniques — Code of practice for protection of personally identifiable information (Pll) in public clouds acting as Pll processors».

ГОСТ ISO/IEC 29100-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных. Межгосударственный стандарт» введен в действие в качестве национального стандарта Российской Федерации 30.11.2021 г. Он идентичен международному стандарту ISO/IEC 29100:2011 «Информационные технологии. Методы и средства обеспечения безопасности. Основы приватности» («Information technology — Security techniques — Privacy framework»).

ГОСТ Р 59407-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных» введен в действие 30.11.2021 г. Он введен впервые и разработан с учетом основных нормативных положений международного стандарта ИСО/МЭК 29101:2018 «Информационные технологии. Методы и средства обеспечения безопасности. Архитектура обеспечения приватности» (ISO/IEC 29101:2018 «Information technology — Security techniques — Privacy architecture framework»).

Стандарт 59407-2021 предоставляет описания высокоуровневой базовой архитектуры и соответствующих мер защиты персональных данных в информационных системах персональных данных (ИСПдн) и учитывает основные положения нормативных правовых актов Российской Федерации.

Описанная в стандарте архитектура защиты персональных данных:

- предоставляет последовательный высокоуровневый подход к реализации мер защиты при обработке персональных данных с использованием средств автоматизации;
- предоставляет руководство по планированию, проектированию и построению архитектур информационных систем персональных данных, которые обеспечивают защиту персональных данных путем контроля за их обработкой, доступом и передачей;
- показывает, как технологии, обеспечивающие конфиденциальность персональных данных действующих субъектов персональных данных, могут использоваться в качестве мер защиты.

Стандарт применим для организаций, участвующих в определении, приобретении, разработке архитектуры, проектировании, тестировании, поддержке, администрировании и эксплуатации информационных систем персональных данных. Основное внимание в нем уделено информационным системам персональных данных, предназначенным для взаимодействия с субъектами персональных данных.

В стандарте введен ряд основных понятий:

Персональные данные (ПДн) — любая информация, относящаяся к прямо или косвенно определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Безопасность персональных данных — состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Информационная система персональных данных (ИСПДн) — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных — обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Обработка персональных данных — 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, уничтожение персональных данных.

Угрозы безопасности персональных данных — совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Предоставление персональных данных — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Базовая архитектура в стандарте представлена следующим образом:

- уровни технической базовой архитектуры, приведенные в разделе 7.2, определяют ее с точки зрения компонентов. В каждом уровне сгруппированы компоненты, имеющие общую цель или сходную функцию;
- модель реализации, приведенная в разделе 7.3, определяет базовую архитектуру с точки зрения автономной ИСПДн. Каждое представление показывает группировку компонентов в зависимости от их реализации в ИСПДн;
- представления, приведенные в разделе 7.4, определяют базовую архитектуру с точки зрения взаимодействия. Эти представления демонстрируют взаимодействие компонентов между системами сторон, участвующих в обмене информацией.

Центральным элементом базовой архитектуры является создаваемая ИСПДн. Сторонами, участвующими в обработке ПДн, являются: субъект персональных данных, оператор персональных данных и обработчик ПДн, которому оператор персональных данных поручает обработку ПДн. С точки зрения реализации базовая архитектура защиты ПДн разделена на три части. Каждая часть относится к реализованной ИСПДн с точки зрения каждого из участников.

В разделе 5 стандарта рассмотрены этапы жизненного цикла персональных данных при обработке: сбор, передача, использование, хранение, уничтожение.

В разделе 6 выделены основные принципы обеспечения безопасности персональных данных:

- согласие и выбор;
- законность цели и ее спецификация;
- ограничение на сбор информации;
- минимизация данных;
- ограничения в отношении использования, хранения и раскрытия;
- точность и качество ПДн;
- открытость, прозрачность и уведомление;
- персонифицированный доступ;
- ответственность;
- обеспечение безопасности информации;
- соответствие требованиям нормативной правовой базы.

Информационные системы персональных данных должны реализовывать меры защиты как основной элемент на каждом этапе жизненного цикла ПДн. Меры защиты подробно описаны в разделе 7 стандарта.

В приложении А содержится примерный перечень значимых вопросов и описание взаимосвязи значимых вопросов с принципами обеспечения безопасности ПДн и компонентами базовой архитектуры защиты ПДн, приведенными в стандарте.

Межгосударственный стандарт ГОСТ ISO/IEC 29100-2021 предоставляет высокоуровневые основы обеспечения безопасности персональных данных 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. В некоторых странах положения этого стандарта, связанные с мерами защиты ПДн, могут расцениваться как уточнение и дополнение к законодательным требованиям обеспечения безопасности ПДн.

В стандарте представлены основы обеспечения безопасности персональных данных, 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.

Стандарт вводит ряд понятий в предметной области:

Согласие на обработку — 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.

Персональные данные:

(а) 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.

Политика обеспечения защиты ПДн — общее намерение и направление деятельности, правила и обязательства, формально выраженные оператором ПДн, касающиеся обработки ПДн в определенной области.

Обработка ПДн — любая операция или совокупность операций, выполняемых в отношении ПДн.

Специальные категории ПДн — 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.

В качестве основы обеспечения защиты ПДн, в стандарте определены следующие компоненты:

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

Указанные компоненты подробно описаны в разделе 4 стандарта. В этом же разделе определены требования к мерам защиты ПДн. Они идентифицируются как часть общего процесса управления рисками обеспечения прав субъектов ПДн, на который оказывают влияние следующие факторы:

- 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;
- факторы бизнеса;
- другие факторы, которые могут влиять на проектирование ИСПДн и связанные с ними требования к мерам обеспечения безопасности ПДн.

В разделе 5 подробно описаны следующие принципы защиты персональных данных:

- согласие и выбор;
- законность цели и ее спецификация;
- ограничение на сбор информации;
- минимизация данных;
- ограничения в отношении использования, хранения и раскрытия;
- точность и качество;
- открытость, прозрачность и уведомление;
- индивидуальное участие и доступ;
- ответственность;
- информационная безопасность;
- соответствие безопасности ПДн.

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27018-2020 разработан для использования организациями в качестве справочника при выборе мер защиты ПДн в процессе реализации системы менеджмента ИБ облачных вычислений на основе ИСО/МЭК 27001, а также в качестве рекомендаций по реализации общепринятых мер защиты ПДн для организаций, выступающих в качестве обработчиков ПДн публичного облака. В частности, стандарт основан на требованиях ИСО/МЭК 27002 с учетом специфической среды риска, возникающей из тех требований по защите ПДн, которые могут быть применимы к поставщикам служб публичных облаков, выступающим в качестве обработчика ПДн.

В случаях, когда для обработки персональных данных используются облачные вычисления, поставщик служб облачных вычислений, действующий на основании соответствующего договора с потребителем, должен организовать свои службы таким образом, чтобы требования законодательства и установленных регуляторами правил в области защиты ПДн соблюдались для обоих участников. Распределение конкретных требований и ответственности за их реализацию между участниками зависит от правовой юрисдикции и условий договора между потребителем и поставщиком. При использовании служб публичного облака, в котором обработка ПДн осуществляется в интересах и в соответствии с инструкциями потребителя служб облачных вычислений, поставщик служб публичного облака выступает в роли обработчика ПДн.

Стандарт имеет структуру, схожую со структурой ИСО/МЭК 27002. В случаях, когда определенные в ИСО/МЭК 27002 цели, меры обеспечения ИБ применимы напрямую, без каких-либо дополнительных особенностей, дается ссылка на ИСО/МЭК 27002. Дополнительные меры обеспечения ИБ и соответствующие им рекомендации по реализации, применимые к защите персональных данных поставщиками служб облачных вычислений, приведены в приложении А. Стандарт должен использоваться вместе с ИСО/МЭК 27001, и применение дополнительных мер обеспечения ИБ, определенных в приложении А, должно рассматриваться как часть процесса внедрения системы менеджмента ИБ на основе 27001.

В соответствующих разделах стандарта подробно описаны меры обеспечения ИБ в соответствии со стандартом 27002:

- политики информационной безопасности;
- организация деятельности по информационной безопасности;
- безопасность, связанная с персоналом;
- менеджмент активов;
- управление доступом;
- криптография;
- физическая безопасность и защита от воздействия окружающей среды;
- безопасность при эксплуатации;
- безопасность систем связи;
- приобретение, разработка и поддержка систем;
- взаимоотношения с поставщиками;
- менеджмент инцидентов информационной безопасности;
- аспекты информационной безопасности в рамках менеджмента непрерывности деятельности организации;
- соответствие.