УТВЕРЖДАЮ

Генеральный директор

ФБУ «Тест- С.-Петербург»

_____ П.Л. Овчаренко

«01» февраля 2022 г.

Политика

Федерального бюджетного учреждения

«Государственный региональный центр

стандартизации, метрологии и испытаний

в г. Санкт-Петербурге и Ленинградской области»

в отношении обработки персональных данных

2022

Содержание

Список терминов и определений

- Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную поддержку выполнения установленных функций.

- Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

- Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

- Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

- 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.

- Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

- Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

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

- Система обеспечения безопасности персональных данных – система правовых, организационных, технических и иных мер по обеспечению доступности, целостности и конфиденциальности персональных данных.

- Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного

государства, иностранному физическому лицу или иностранному юридическому лицу.

- Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1. Общие положения

1.1. Настоящий документ определяет политику обработки и защиты персональных данных (далее – ПДн) в Федеральном бюджетном учреждении «Государственный региональный центр стандартизации, метрологии и испытаний в г. Санкт-Петербурге и Ленинградской области» (далее – Оператор).

Настоящая Политика разработана с учётом положений нормативных документов, регламентирующих порядок обеспечения безопасности ПДн, указанных в пункте 19 настоящей Политики.

1.2. Целью настоящей Политики являются определение особенностей обработки и обеспечения безопасности ПДн, а также минимизация ущерба, который может возникнуть вследствие воздействия угроз информационной безопасности, приводящих к нарушению требуемых свойств безопасности ПДн и обеспечения защиты прав и свобод субъекта ПДн при обработке его ПДн.

1.3. Организация обработки и обеспечения безопасности ПДн осуществляется в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - ФЗ «О персональных данных») и принятыми в соответствии с ним нормативными правовыми актами.

1.4. Настоящая Политика распространяется на все технологические процессы Оператора, связанные с обработкой ПДн субъектов, и обязательна для применения всеми работниками Оператора.

1.5. Работники Оператора должны быть ознакомлены с внутренними нормативными документами, устанавливающими правила обработки и обеспечения безопасности ПДн, в соответствии с порядком, изложенным в этих внутренних нормативных документах. Контроль за ознакомлением осуществляют руководители структурных подразделений.

1.6. Требования настоящей Политики при необходимости могут детализироваться иными внутренними нормативными документами Оператора.

2. Перечень действий с персональными данными

При обработке ПДн Оператор будет осуществлять следующие действия с ПДн: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

3. Состав обрабатываемых персональных данных

3.1. Обработке Оператором подлежат ПДн следующих субъектов ПДн:

- работники Оператора;
- контрагенты Оператора;
- физические лица, обратившиеся к Оператору в порядке, установленном Федеральным законом от 02.05.2006 № 9-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

3.2. Состав ПДн каждой из перечисленных в пункте 3.1 настоящей Политики категории субъектов определяется согласно нормативным документам, перечисленным в разделе 19 настоящей Политики, а также нормативным документам Оператора, изданным для обеспечения их исполнения.

3.3. В случаях, предусмотренных действующим законодательством, субъект ПДн принимает решение о предоставлении его ПДн Оператору и дает согласие на их обработку свободно, своей волей и в своём интересе.

3.4. Оператор обеспечивает соответствие содержания и объема обрабатываемых ПДн заявленным целям обработки и, в случае необходимости, принимает меры по устранению их избыточности по отношению к заявленным целям обработки.

3.5. Обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, Оператор не осуществляет.

4. Цели обработки персональных данных

ПДн Оператор обрабатывает в следующих целях:

4.1. осуществление и выполнение возложенных действующим законодательством на Оператора функций, полномочий и обязанностей, в частности выполнение требований законодательства по определению порядка обработки и защиты ПДн граждан, являющихся работниками или контрагентами Оператора (далее – субъекты ПДн);

4.2. осуществления прав и законных интересов Оператора в рамках осуществления видов деятельности, предусмотренных Положением об Операторе, иными локальными нормативными актами Оператора, или третьих лиц, либо достижения общественно значимых целей;

4.3. в иных законных целях.

5. Цели обеспечения безопасности персональных данных

Целями обеспечения безопасности ПДн являются:

– выполнение требований законодательства Российской Федерации в отношении обеспечения безопасности ПДн, выполнение требований внутренних нормативных документов и/или обязательств Оператора перед контрагентами и законодательством Российской Федерации в отношении обеспечения информационной безопасности;

– обеспечение конфиденциальности ПДн и информации, определенной в документе Оператора, регламентирующем перечень информации конфиденциального характера;

– обеспечение целостности ПДн, иной конфиденциальной информации и средств автоматизации;

– обеспечение доступности ПДн и иной конфиденциальной информации в соответствии с правилами разграничения доступа к информации;

– обеспечение достоверности ПДн и иной конфиденциальной информации;

– обеспечение своевременности поступления информации из/в информационных (ые) систем(ы) ПДн (далее – ИСПДн);

– предотвращение и (или) снижение возможного ущерба от инцидентов информационной безопасности;

– повышение уровня стабильности и непрерывности функционирования ИСПДн;

– обеспечение адекватного времени восстановления штатного функционирования ИСПДн в случае прерывания такого функционирования.

6. Общие положения по организации обработки и обеспечению безопасности персональных данных

6.1. Основными принципами обработки ПДн у Оператора являются:

– законность целей и способов обработки ПДн и добросовестность Оператора, как оператора, что достигается путём установления требований к обработке ПДн и неукоснительного их соблюдения;

– соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн;

– соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;

– достоверность ПДн, их достаточность для целей обработки, недопустимость обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;

– недопустимость объединения созданных для несовместимых между собой целей баз данных ИСПДн;

– хранение ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, и уничтожение ПДн по достижении целей обработки или в случае утраты необходимости в их достижении.

6.2. Оператор как оператор, осуществляет обработку ПДн физических лиц в рамках требований законодательства Российской Федерации в целях:

– оказания услуг контрагентам Оператор, исполнения договоров, сторонами которых являются субъекты ПДн, при этом ПДн субъектов не распространяются, а также не предоставляются третьим лицам без согласия

субъектов ПДн и используются у Оператора исключительно для исполнения указанных договоров;

– выполнения трудового законодательства Российской Федерации.

6.3. Оператор обрабатывает ПДн, осуществляя свою деятельность в соответствии с требованиями Гражданского кодекса Российской Федерации, Трудового кодекса Российской Федерации, Налогового кодекса Российской Федерации, федеральных законов, Положения об Операторе.

6.4. Обработка ПДн у Оператора осуществляется следующими способами:

– неавтоматизированная обработка ПДн;

– автоматизированная обработка ПДн с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;

– смешанная обработка ПДн.

6.5. В соответствии со степенью тяжести последствий потери свойств безопасности ПДн для субъектов ПДн Оператор выделяет следующие категории ПДн:

– ПДн, отнесённые в соответствии с ФЗ «О персональных данных» к иным ПДн;

– ПДн, отнесённые в соответствии с ФЗ «О персональных данных» к общедоступным ПДн.

6.6. В случае достижения цели обработки ПДн, если иное не предусмотрено законодательством Российской Федерации, Оператор прекращает обработку и производит их уничтожение, или обеспечивает прекращение обработки и уничтожение ПДн, которые обрабатывались третьими лицами на основании договора с Оператором, в порядке, установленном законодательством Российской Федерации. Уничтожение ПДн и материальных носителей ПДн у Оператора осуществляется в согласованном с назначаемым приказом Оператора ответственным лицом (далее – Ответственное лицо) порядке и документируется. Детально соответствующий порядок определяется в иных внутренних документах, регламентирующих порядок уничтожения информации, в отношении которой установлено требование обеспечения конфиденциальности, и материальных носителей такой информации.

6.7. Ответственное лицо определяет необходимость направления в уполномоченный орган по защите прав субъектов ПДн уведомления об обработке (о намерении осуществлять обработку) ПДн в соответствии с требованиями законодательства Российской Федерации. В случае установления необходимости направления такого уведомления, ответственным за его составление, направление, уточнение и изменение является Ответственное лицо (ответственное подразделение).

7. Основные требования к процедурам обработки персональных данных

7.1. Обработка ПДн у Оператора должна осуществляться с согласия субъекта ПДн, кроме случаев, установленных законодательством Российской Федерации, когда такое согласие не требуется.

7.2. У Оператора запрещается принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн, или иным образом затрагивающих его права и законные интересы, кроме случаев и условий, предусмотренных законодательством Российской Федерации.

7.3. Оператор не осуществляет трансграничную передачу ПДн.

7.4. Предоставление ПДн Оператором третьему лицу, кроме случаев, предусмотренных законодательством Российской Федерации, должно осуществляться с согласия субъекта ПДн. В случае, если Оператор на основании договора поручает обработку ПДн третьему лицу, существенным условием договора (или заключенного с таким лицом соглашения о конфиденциальности) должна являться обязанность указанного лица по обеспечению конфиденциальности ПДн и безопасности ПДн при их обработке, а также выполнение им требований, предъявляемых к защите ПДн в соответствии со статьей 19 ФЗ «О персональных данных», и несение ответственности перед Оператором за обработку таких ПДн.

7.5. Руководители подразделений Оператора, обеспечивающих достижение целей обработки ПДн, готовят проекты утверждаемых в установленном порядке документов, устанавливающих для каждой такой цели:

– объем и содержание ПДн;

– сроки обработки ПДн, в том числе сроки хранения;

– правовые основания для обработки ПДн, в том числе необходимость, форму и порядок получения согласия субъектов ПДн;

– источники получения ПДн, виды и способы обработки ПДн, состав получателей (пользователей) ПДн.

7.6. В случаях, установленных законодательством Российской Федерации, обработка ПДн у Оператора осуществляется с согласия субъекта ПДн в письменной форме, оформляемого в соответствии с требованиями статьи 9 ФЗ «О персональных данных».

7.7. Рекомендации к порядку получения согласия субъекта ПДн и требования к виду и составу такого согласия устанавливаются в иных внутренних документах.

7.8. У Оператора ведется учёт работников, осуществляющих обработку ПДн, в том числе с использованием ИСПДн. Учёт ведется на основе списков доступа работников.

7.9. Работники Оператора, осуществляющие обработку ПДн в ИСПДн, должны быть проинформированы о факте обработки ими ПДн и категориях обрабатываемых ПДн при предоставлении доступа к ИСПДн, а также должны быть ознакомлены под личную подпись со всей содержащейся в должностных инструкциях и соответствующих внутренних документах совокупностью требований Оператора по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей.

7.10. Во избежание несанкционированного доступа к ПДн рекомендуется:

– исключать фиксацию на одном материальном носителе ПДн и иной информации (в т.ч. других ПДн), если материальный носитель не позволяет осуществлять обработку ПДн отдельно от другой зафиксированной на том же носителе информации (ПДн);

– для каждой категории ПДн использовать отдельный материальный носитель.

7.11. При обработке ПДн на бумажных носителях следует руководствоваться «Положением об особенностях обработки ПДн, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства Российской Федерации от 15.09.2008 № 687.

8. Принципы реализации политики защиты персональных данных

8.1. Принцип законности. Обязательный учёт и выполнение требований нормативных правовых актов Российской Федерации в области безопасности ПДн.

8.2. Принцип единства и унификации. Единство подходов к обеспечению информационной безопасности, определению и реализации стратегии противодействия потенциальным угрозам.

8.3. Принцип разумной достаточности. Используемые меры и средства обеспечения безопасности ПДн не должны ухудшать основные технические характеристики информационных и автоматизированных систем Оператора и должны проходить проверку на избыточность и достаточность.

8.4. Принцип оптимальности. Обеспечение необходимого уровня защиты ПДн при минимальных финансовых затратах.

8.5. Принцип непрерывности защиты. Обеспечение защиты ПДн на всех этапах обработки и во всех режимах функционирования ИСПДн, в том числе при проведении модернизации, ремонтных и регламентных работ.

8.6. Принцип превентивности. Предполагает направленность методов обеспечения безопасности ПДн на минимизацию возможности реализации угроз и снижения рисков информационной безопасности, а не на компенсацию их последствий.

8.7. Принцип преемственности. Требует непрерывного совершенствования системы защиты на основе уже используемых организационных и технических мер с учётом применения перспективных отечественных и зарубежных методик и технических средств защиты.

8.8. Принцип комплексности. Комплексный подход к построению и реализации методов защиты ПДн и обеспечения информационной безопасности.

8.9. Общие принципы построения системы защиты указанные в настоящем разделе приведены в порядке их значимости (8.1 – самый значимый, 8.8 – наименее значимый). С учётом приведённых принципов обеспечения информационной безопасности, а также с учётом их иерархии выбираются методы, средства и механизмы обеспечения безопасности ПДн.

9. Основные задачи обеспечения безопасности ПДн

9.1. Идентификация вероятных угроз.

Для достижения указанных целей на каждой стадии жизненного цикла ИСПДн должны быть выявлены, учтены и документированы источники угроз и угрозы безопасности ИСПДн, вероятность реализации угроз и вероятный ущерб в результате реализации угроз безопасности. На основе полученных данных разрабатывается модель угроз и модель нарушителя.

9.2. Разработка требований и технических решений.

Должны быть определены и документированы требования и решения по обеспечению информационной безопасности на основе модели угроз и модели нарушителя.

9.3. Реализация.

Должны быть реализованы и документированы принятые организационно-технические меры по обеспечению информационной безопасности.

9.4. Контроль.

Должен обеспечиваться непрерывный контроль, противодействие и предупреждение попыток и выявленных фактов несанкционированных (неправомерных) действий, направленных на нарушение конфиденциальности, целостности, доступности, достоверности ПДн, иной защищаемой информации обрабатываемой ИСПДн, непрерывности функционирования ИСПДн и снижения экономической эффективности деятельности Оператора.

9.5. Выполнение требований законодательства.

Должны приниматься меры к недопущению использования ПДн в нарушение требований законодательства Российской Федерации.

10. Основные угрозы безопасности персональных данных

10.1. Источники угроз могут быть как внешними, так и внутренними по отношению к ПДн и ИСПДн Оператора. Источниками угроз информационной безопасности ИСПДН являются:

10.1.1. Угрозы, обусловленные действиями субъекта (антропогенные источники угроз):

– внешние антропогенные источники: конкуренты, террористические организации и криминальные структуры, недобросовестные партнеры, разведывательные службы иностранных государств и т.д.;

– внутренние антропогенные источники: работники, получившие легальный доступ в ИСПДн, а также легальный доступ в контролируемую зону (далее – КЗ), работники, имеющие легальный доступ в КЗ, но не имеющие доступ в ИСПДн , работники, имеющие легальный доступ в ИСПДн, но не имеющие доступ в КЗ.

10.1.2. Угрозы, обусловленные техническими средствами (техногенные источники угроз):

– внешние: аппаратные, программные, программно-аппаратные средства различного назначения, использующие различные каналы доступа к ИСПДн;

– внутренние: аппаратные, программные, программно-аппаратные средства различного назначения.

10.1.3. Угрозы, обусловленные стихийными бедствиями (стихийные источники угроз):

– пожары, наводнения, землетрясения и пр.

10.1.4. Основными угрозами информационной безопасности в ИСПДн являются:

– несанкционированный доступ (НСД) к информации, обрабатываемой в ИСПДн и передаваемой по каналам передачи данных;

– нарушение функционирования ИСПДн или отдельных ее элементов.

10.2. Цели реализации угроз. В результате реализации угроз информационной безопасности в ИСПДн могут быть нарушены:

– конфиденциальность (утечка, перехват, съём, копирование, хищение, разглашение) информации;

– целостность (утрата, уничтожение, модификация) информации;

– доступность (блокирование) информации и отдельных элементов ИСПДн;

– достоверность и непротиворечивость информации (фальсификация);

– непрерывность и стабильность функционирования ИСПДн.

11. Основные направления и меры защиты персональных данных

11.1. Объектами защиты являются ПДн и информационные технологические процессы, обрабатывающие ПДн.

11.2. Безопасность ПДн достигается путем реализации комплекса мероприятий, позволяющих минимизировать риск нарушения информационной безопасности. Безопасность ПДн при их обработке в ИСПДн Оператора обеспечивается с помощью системы защиты ПДн. Система защиты ПДн включает организационные и (или) технические меры, определенные с учётом актуальных угроз безопасности ПДн и информационных технологий, используемых в ИСПДн.

11.3. При обработке ПДн Оператор обеспечивает их безопасность и принимает необходимые организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий, путём установления в отношении таких данных режима конфиденциальности и контроля за его соблюдением, а также путём внедрения дополнительных мер защиты, реализующих требования законодательства Российской Федерации и принятых в соответствии с ним нормативных правовых актов и стандартов.

11.4. При обеспечении защиты ПДн Оператор руководствуется требованиями законодательства Российской Федерации. В качестве базовой модели угроз безопасности ПДн принята «Частная модель угроз ИСПДн».

11.5. Все разрабатываемые у Оператора и касающиеся обработки и/или защиты ПДн проекты документов должны быть согласованы с Ответственным

лицом (подразделением). Также обязательному согласованию с Ответственным лицом (подразделением) подлежат мероприятия по сбору и защите ПДн.

11.6. У Оператора в установленном порядке создаётся комиссия по определению требуемого уровня защищённости ПДн при их обработке в ИСПДн. В функции комиссии входит определение требуемого уровня защищённости ПДн при их обработке в ИСПДн, а также утверждение актов определения требуемого уровня защищённости ПДн при их обработке в ИСПДн. Ответственное лицо (подразделение) ведёт перечень обрабатывающих ПДн на основе обследования автоматизированных систем Оператора и перечень ИСПДн на основе утвержденных актов определения требуемого уровня защищённости ПДн при их обработке в ИСПДн Оператора.

11.7. Для каждой ИСПДн определяется и фиксируется в Акте определения требуемого уровня защищенности ПДн при их обработке в ИСПДн:

– цели обработки ПДн;

– объём и содержание обрабатываемых ПДн, соответствующие целям обработки;

– перечень действий с ПДн и способы их обработки для достижения указанных целей.

11.8. Выбор требований по обеспечению безопасности ПДн осуществляется в соответствии с требованиями законодательства Российской Федерации в зависимости от установленного уровня защищённости ПДн, зафиксированного в соответствующем Акте определения требуемого уровня защищенности ПДн при их обработке в ИСПДн и в соответствии с частной моделью угроз безопасности ПДн Оператора.

11.9. В документации на внедряемые ИСПДн Оператора должны быть отражены вопросы обеспечения безопасности обрабатываемых ПДн.

11.10. Ответственное лицо (подразделение) должно:

– разработать систему обеспечения безопасности ПДн, обеспечивающую нейтрализацию предполагаемых угроз, при этом ввод в эксплуатацию и использование средств и систем защиты информации должны осуществляться в соответствии с документацией на них;

– осуществлять проверку готовности средств защиты информации, а также контроль их использования;

– проводить анализ происходящих нарушений порядка обработки и защиты ПДн, разработку и принятие мер по предотвращению возможных опасных последствий;

– совместно с подразделением по работе с персоналом проводить обучение лиц, использующих средства защиты информации, применяемые в ИСПДн, правилам работы с ними;

11.11. Требования по обеспечению безопасности информации в ИСПДн средствами антивирусной защиты и порядок проведения контроля реализации этих требований установлены в соответствующих внутренних документах.

11.12. У Оператора вводятся ограничения на доступ в помещения, в которых проводится обработка ПДн, и устанавливаются требования к учёту, хранению и уничтожению материальных носителей ПДн в соответствующих внутренних документах.

11.13. Обеспечение конфиденциальности ПДн не требуется в случае обезличивания ПДн и в отношении общедоступных ПДн.

11.14. Координацию работ по созданию системы обеспечения безопасности ПДн и взаимодействие с регуляторами по вопросам безопасности ПДн у Оператора осуществляет Ответственное лицо (подразделение). Ответственное лицо (руководитель ответственного подразделения) является ответственным за организацию обработки ПДн.

11.15. Обеспечение информационной безопасности ПДн и ИСПДн осуществляется по следующим направлениям, реализуемым организационно-техническими мерами защиты:

11.15.1 организационно-распорядительные меры;

11.15.2. меры физической защиты;

11.15.3. технические меры:

– реализация подсистемы сетевой безопасности;

– реализация подсистемы контроля и управления доступом;

– реализация подсистемы регистрации и учёта;

– реализация подсистемы обеспечения целостности;

– реализация подсистемы защиты от вредоносного программного обеспечения (кода);

– реализация подсистемы криптографической защиты;

– реализация подсистемы контроля защищенности;

– реализация подсистемы обновления активов программного обеспечения;

– реализация подсистемы резервирования и отказоустойчивости;

– реализация подсистемы централизованного управления и мониторинга.

11.15.4. Организационно-распорядительные меры:

– на всех стадиях жизненного цикла ИСПДн, все технические и организационные решения по созданию, модернизации ИСПДн, предоставлению доступа к ИСПДн и прочие решения, прямо или косвенно связанные с информационной безопасностью ИСПДн, должны согласовываться со службой защиты информации Оператора;

– идентификация и классификация объектов защиты;

– учёт объектов защиты. Все основные объекты защиты (информационные, программные, аппаратные активы и др.) должны быть учтены и документированы, должно быть определено их местоположение;

– документальное оформление перечня сведений конфиденциального характера и/или коммерческой тайны и иной защищаемой информации;

– разработка модели угроз и модели нарушителя информационной безопасности ИСПДн, оценка рисков и разработка проектных решений по обеспечению информационной безопасности;

– ограничение доступа персонала и посторонних лиц в помещения, где размещены средства информатизации и коммуникации, а также где хранятся носители информации;

– реализация разрешительной системы допуска пользователей и обслуживающего персонала к информации, техническим средствам и связанным с их использованием работам, документам;

– разработка и внедрение матриц доступа субъектов доступа ИСПДн к информационным ресурсам, программным, программно-аппаратным средствам обработки (передачи) данных и средствам защиты информации;

– разработка нормативных документов, регламентирующих правила выполнения технологических операций в ИСПДн, с учётом требований информационной безопасности;

– персональная ответственность лиц, допущенных к ИСПДн за соблюдение ими установленного у Оператора порядка обеспечения информационной безопасности (для получения доступа к ИСПДн обслуживающий персонал должен изучить требования нормативных документов по защите информации, действующих у Оператора).

11.15.5. Меры физической защиты:

– организация физической охраны зданий, сооружений и помещений с помощью сил охраны и технических средств, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц с целью деструктивных воздействий на ИСПДн, хищения документов и информационных носителей, самих средств информатизации, исключающих нахождение внутри контролируемой зоны технических средств деструктивного воздействия, разведки или промышленного шпионажа;

– организация физической защиты технических средств обработки, хранения и передачи информации.

Технические меры обеспечения информационной безопасности (приведены типовые подходы, детальные требования) определяются и уточняются на основе модели угроз):

11.15.6. реализация подсистемы контроля и управления доступом, в том числе:

– идентификация и аутентификация;

– управление доступом к объектам защиты на базовом, системном, прикладном и сетевом уровнях;

– контроль доступа к персональным компьютерам, серверам, информационным ресурсам, сетевому оборудованию и прочим объектам защиты;

– контроль использования внешних (в т.ч. съёмных) носителей информации;

– контроль использования мобильных устройств;

11.15.7. реализация подсистемы регистрации и учёта;

11.15.8. реализация подсистемы защиты от вредоносного программного обеспечения (кода);

11.15.9. реализация подсистемы обеспечения целостности технических, программных и информационных ресурсов;

11.15.10. реализация подсистемы обновления активов программного обеспечения;

11.15.11. реализация подсистемы сетевой безопасности;

11.15.12. реализация подсистемы контроля защищённости;

11.15.13. реализация подсистемы криптографической защиты;

11.15.14. реализация подсистемы централизованного управления и мониторинга системы защиты информации;

11.15.15. реализация подсистемы резервирования и отказоустойчивости.

12. Основные мероприятия по обеспечению прав субъектов персональных данных при обработке их персональных данных

12.1. Субъект ПДн, обрабатываемых Оператором, имеет право:

– на получение сведений об Операторе как об операторе ПДн, о месте нахождения Оператора, о наличии у Оператора ПДн, относящихся к соответствующему субъекту ПДн, а также на ознакомление с такими ПДн;

– требовать от Оператора уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

– принимать предусмотренные законодательством Российской Федерации меры по защите своих прав.

12.2. Оператор в обязательном порядке рассматривает все обращения субъектов ПДн, в том числе, если субъект ПДн считает, что Оператор

осуществляет обработку его ПДн с нарушением требований законодательства Российской Федерации или иным образом нарушает его права и свободы.

12.3. Порядок обработки обращений и запросов субъектов ПДн (или их законных представителей) по вопросам обработки их ПДн и действий в случае запросов уполномоченного органа по защите прав субъектов ПДн или иных надзорных органов, осуществляющих контроль и надзор в области ПДн, устанавливается во внутренних документах, разрабатываемых Ответственным лицом (подразделением) в соответствии с настоящей Политикой.

12.4. Отказ субъекта предоставить свои ПДн Оператору для обработки в определенных целях влечет невозможность достижения этих целей.

12.5. Предоставление ПДн не должно нарушать конституционные права и свободы других лиц, в т.ч. работников Оператора и в предоставляемых данных не должны содержаться ПДн, относящиеся к другим субъектам ПДн.

12.6. В случае отзыва субъектом ПДн согласия на обработку его ПДн, если иное не предусмотрено законодательством Российской Федерации, Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если ПДн обрабатываются третьими лицами по договору с Оператором). В случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если ПДн обрабатываются третьими лицами по договору с Оператором) в порядке, установленном законодательством Российской Федерации о защите ПДн.

13. Обязанности работников, допущенных к обработке персональных данных

13.1. Работники, допущенные к обработке ПДн, обязаны:

– знать и неукоснительно выполнять требования настоящей Политики;

– обрабатывать ПДн только в рамках выполнения своих должностных обязанностей;

– не разглашать ПДн, полученные в результате выполнения своих должностных обязанностей, а также ставшие им известными по роду своей деятельности;

– пресекать действия других лиц, которые могут привести к разглашению (уничтожению, искажению) ПДн;

– выявлять факты разглашения (уничтожения, искажения) ПДн и информировать об этом Ответственное лицо (подразделение).

13.2. Обязанности работников, допущенных к обработке ПДн, регламентируются внутренними документами, устанавливающими правила обращения с конфиденциальной информацией у Оператора.

14. Контроль за соблюдением требований настоящей Политики

Контроль за обеспечением безопасности ПДн и соблюдением требований настоящей Политики осуществляет Ответственное лицо (подразделение).

15. Ответственность за несоблюдение положений настоящей Политики

Ответственность работников Оператора за несоблюдение требований настоящей Политики, повлекшее за собой разглашение, утрату или нарушение целостности ПДн, определяется законодательством Российской Федерации, внутренними документами, а также трудовыми договорами и должностными инструкциями работников Оператора.

16. Порядок пересмотра Политики

16.1. Настоящая Политика пересматривается с периодичностью не реже чем 1 раз в 2 года. При пересмотре Политики учитываются результаты контроля эффективности обеспечения информационной безопасности за предыдущий период.

16.2. Процедура пересмотра Политики включает:

– анализ и выявление несоответствий действующей Политики текущим условиям;

– анализ инцидентов информационной безопасности и принятых корректирующих мер;

– разработку предложений по совершенствованию Политики;

– согласование и утверждение новой редакции Политики.

16.3. При осуществлении процедуры пересмотра учитываются:

– результаты контроля состояния информационной безопасности и отзывы заинтересованных сторон о состоянии информационной безопасности в ИСПДн;

– изменения в организационно-штатной структуре Оператора;

– изменения в структурах и конфигурациях применяемых ИСПДн;

– изменения в законодательной и нормативной базе по информационной безопасности;

– результаты анализа произошедших инцидентов информационной безопасности, а также вновь выявленные уязвимости и угрозы ИСПДн;

– изменения в управлении информационной безопасностью, включая изменения в распределении ресурсов и обязанностей при обеспечении информационной безопасности.

–

17. Аудит безопасности персональных данных

17.1. У Оператора должно быть регламентировано регулярное проведение внутреннего аудита информационной безопасности ИСПДн на соответствие требованиям настоящей Политики.

17.2. Аудит информационной безопасности ИСПДн должен проводиться с периодичностью не реже чем 1 раз год.

17.3. Для проведения аудита информационной безопасности ИСПДн должна разрабатываться программа и методика проведения аудита, основанная на требованиях настоящей Политики.

17.4. Результаты проведения аудита информационной безопасности должны фиксироваться в протоколах проведения аудита информационной безопасности ИСПДн.

17.5. По результатам проведения аудита в кратчайшие сроки должны приниматься меры по устранению выявленных несоответствий и нарушений.

18. Заключительные положения

18.1. Руководители подразделений осуществляют ознакомление работников подразделений с настоящей Политикой под личную подпись и обеспечивают хранение подписанных листов ознакомления, их сканирование и направление отсканированных копий Ответственному лицу (в Ответственное подразделение). Ознакомление вновь принимаемых работников с настоящей Политикой осуществляет отдел по работе с персоналом.

18.2. Ответственность за поддержание настоящей Политики в актуальном состоянии возлагается на Ответственное лицо (руководителя Ответственного подразделения).

18.3. В случае изменения законодательства Российской Федерации и принятых в соответствии с ним нормативных правовых актов, изменения или введения в действие стандартов, нормативных методических рекомендаций, требований уполномоченных органов настоящая Политика применяется в части, не противоречащей вновь принятым нормативным правовым документам. При необходимости Ответственное лицо (подразделение) незамедлительно инициирует внесение соответствующих изменений в настоящую Политику.

18.4. Внесение изменений в настоящую Политику должно осуществляться на периодической и внеплановой основе:

– периодическое внесение изменений не реже одного раза в 3 года;

– внеплановое внесение изменений может производиться в случае изменения законодательства Российской Федерации и принятых в соответствии с ним нормативных правовых актов.

19. Перечень нормативных документов

Обработка ПДн осуществляется на основе следующих федеральных законов и нормативных правовых актов:

1) Конституции Российской Федерации;

2) Трудового кодекса Российской Федерации;

3) Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

4) Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

5) Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

6) Постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

7) Приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

8) Приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

9) Приказа Роскомнадзора от 05 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

10) Иных нормативных правовых актов Российской Федерации и нормативных документов уполномоченных органов государственной власти.