



**АКЦИОНЕРНОЕ ОБЩЕСТВО
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ И КОМПЛЕКСОВ СВЯЗИ
«НЕПТУН»**

**ПОЛИТИКА
в отношении обработки персональных данных**

**Акционерного общества
«Научно-исследовательский институт
автоматизированных систем и комплексов связи «Нептун»
(АО «НИИ «Нептун»)**

Оглавление

1.	Введение.....	3
2.	Обозначения и сокращения.....	3
3.	Термины и определения.....	4
4.	Основания для разработки.....	6
5.	Содержание политики.....	7
6.	Ответственность за нарушение правил обработки персональных данных.....	10
7.	Контроль обработки персональных данных.....	11
8.	Внесение изменений и дополнений.....	11
9.	Заключительные положения	11

1. Введение

1.1 Политика АО «НИИ «Нептун» в отношении обработки персональных данных (далее – Политика) определяет систему взглядов на процесс обработки персональных данных и содержит сведения о реализуемых требованиях к обработке и защите персональных данных. Политика представляет собой систематизированное изложение целей и задач защиты персональных данных при их обработке в АО «НИИ «Нептун» (далее – Общество).

1.2 Целью настоящей Политики является информирование субъектов персональных данных и лиц, участвующих в обработке персональных данных, о соблюдении в Обществе основополагающих принципов законности, справедливости, соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки.

1.3 Область применения настоящей Политики охватывает персональные данные, получаемые, создаваемые, передаваемые, хранимые и обрабатываемые с использованием информационных систем персональных данных (далее – ИС ПДн) и систем бумажного документооборота, а также сами системы и информационную инфраструктуру, владельцем и пользователем которых является Общество.

1.4 Требования настоящей Политики обязательны для исполнения работниками всех подразделений Общества (штатных, временных и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.), на постоянной или временной основе имеющих доступ к персональным данным работников Общества. Политика действует в отношении всех персональных данных, обрабатываемых в Обществе, и является общедоступным документом.

1.5 Настоящая Политика вводится в действие с момента её утверждения временным генеральным директором Общества и действует в совокупности с дополняющими и изменяющими её документами до выпуска их новых версий. Официальная актуальная версия Политики размещена на сайте Общества www.niineptun.ru. Сделанные с неё бумажные копии являются неконтролируемыми, их актуальность Обществом не поддерживается.

2. Обозначения и сокращения

АС	Автоматизированная система
ИС	Информационная система
ИС ПДн	Информационная система персональных данных
Общество	Акционерное общество «НИИ «Нептун»
ОКБ	Отдел комплексной безопасности
ОРП	Отдел по работе с персоналом
ПДн	Персональные данные
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

3. Термины и определения

3.1 В настоящей Политике применяются следующие термины и определения:

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

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Документированная информация – зафиксированная на материальном носителе информация с реквизитами, позволяющими определить такую информацию или, в установленных законодательством Российской Федерации случаях, ее материальный носитель.

Доступ к информации – возможность получения информации и ее использования.

Доступность информации – состояние, характеризующееся способностью ИС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию и средства доступа к ней.

Информация – сведения (сообщения, данные и т.д.) о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационная безопасность – защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры.

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.

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

Несанкционированный доступ – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор 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.

Политика – общие цели и указания, формально выраженные руководством.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Разглашение информации – действие или бездействие, в результате которых информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Субъект персональных данных - физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Третья сторона – юридическое или физическое лицо, не принадлежащее к кругу

лиц, вовлеченных в определенную проблему или вопрос.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Физические меры защиты – разного рода механические, электро- или электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам АС и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.

4. Основания для разработки

4.1 Настоящая Политика разработана с учётом требований Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации в области персональных данных. При написании отдельных положений использовались следующие нормативные документы:

- Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон);
- Федеральный закон от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»;
- Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ глава 14 «Защита персональных данных работника»;
- Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Постановление Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Рекомендации Роскомнадзора по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

5. Содержание политики

5.1 Общие положения

5.1.1 Общество является Оператором персональных данных. Обработка персональных данных в Обществе включает в себя сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

5.1.2 В рамках Общества создаются, хранятся и обрабатываются ПДн, получаемые непосредственно от работников Общества (штатных, временных и т.п.), в ходе взаимодействия с контрагентами, партнерами, поставщиками услуг и государственными органами и иными лицами.

5.1.3 ПДн могут существовать в разных формах представления: напечатаны или написаны на бумаге, сохранены в электронном виде, переданы по почте, электронными средствами или в устной форме. Не зависимо от того, в каком виде обрабатываются или хранятся ПДн, Общество должно всегда защищать их критичные свойства, такие как конфиденциальность, целостность и доступность.

5.1.4 В целях реализации Политики, в Обществе разрабатываются соответствующие локальные нормативные акты, в том числе:

- Положение об обработке и защите персональных данных в АО «НИИ «Нептун»;
- Перечень персональных данных, обрабатываемых в АО «НИИ «Нептун»;
- Перечень мест хранения материальных носителей персональных данных, обрабатываемых в АО «НИИ «Нептун»;
- Перечень подразделений и должностей работников АО «НИИ «Нептун», допущенных к работе с персональными данными;
- иные сопутствующие документы, регламентирующие вопросы обработки персональных данных в Обществе.

5.1.5 Обработка ПДн, в зависимости от преследуемых целей, осуществляется с согласия Субъектов персональных данных, на обработку предоставляемых ПДн.

5.2 Цели и применяемые способы обработки персональных данных

5.2.1 Основными целями обработки персональных данных в Обществе являются:

- контроль выполняемой работы, соблюдения норм трудового законодательства и иных норм трудового права;
- защита прав и законных интересов Общества и его работников, обеспечение гарантий, безопасности и иных интересов работников Общества;
- предотвращение конфликтов интересов;
- соблюдение законодательства Российской Федерации в различных сферах деятельности;
- ведение договорной и финансово-закупочной деятельности;
- обеспечение пропускного и внутриобъектового режимов.

5.2.2 Для достижения поставленных целей решаются следующие задачи:

- своевременное прогнозирование, выявление и оценка источников угроз ИС ПДн;
- функционирование механизма оперативного реагирования на угрозы ПДн и инциденты с ПДн;

- организация и бесперебойное функционирование делопроизводства;
- защита от вмешательства посторонних лиц в процесс обработки ПДн;
- соответствие мер защиты ПДн, требованиям Федерального законодательства, нормативно-методических документов и договорным обязательствам в части работы с ПДн;
- контроль соблюдения работниками требований нормативных распорядительных документов Общества;
- определение принципов и подходов по совершенствованию организационно-технических мер и механизмов работы с ПДн в Обществе.

5.2.3 Обработка персональных данных в Обществе осуществляется как с использованием средств автоматизации, в том числе в ИС ПДн, так и без использования таких средств (неавтоматизированная и смешанная обработка персональных данных).

5.2.4 В Обществе не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

5.3 Сроки обработки и хранения персональных данных

5.3.1 Обработка ПДн начинается не ранее возникновения правовых оснований для их обработки, определенных нормативными актами, указанными в пункте 4 настоящей Политики.

5.3.2 Обработка ПДн прекращается при достижении целей обработки, утрате правовых оснований обработки, окончании сроков хранения документов, установленных законодательством об архивном деле в Российской Федерации и локальными нормативными актами Общества.

5.3.3 По истечении срока обработки ПДн уничтожаются или обезличиваются для использования в статистических или иных исследовательских целях.

5.4 Права субъектов персональных данных

5.4.1 При обработке ПДн в Обществе устанавливаются следующие категории субъектов персональных данных относятся:

- работники Общества, бывшие работники, кандидаты на замещение вакантных должностей, родственники работников;
- клиенты и контрагенты Общества (физические лица);
- представители (работники) клиентов и контрагентов Общества (юридических лиц).

Все субъекты ПДн имеют право на получение сведений об обработке их ПДн, включая право на получение копий любых записей, содержащих такие ПДн, в порядке и в сроки, предусмотренные Федеральным законом.

5.4.2 Субъект ПДн вправе требовать от Общества уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные Федеральным законом меры по защите своих прав.

5.4.3 Права субъекта на доступ к его ПДн могут быть ограничены в соответствии с Федеральным законом.

5.4.4 Принятие решений, на основании исключительно автоматизированной обработки ПДн, порождающих юридические последствия в отношении субъекта

персональных данных или иным образом затрагивающих его права и законные интересы, допускается с согласия субъекта в письменной форме.

Субъект ПДн имеет право на отзыв своего согласия на обработку персональных данных, выданного ранее.

5.4.5 Если субъект ПДн считает, что Общество осуществляет обработку его ПДн с нарушением требований Федерального закона или иным образом нарушает его права и свободы, он вправе обжаловать действия или бездействие Общества в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

5.4.6 Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

5.5 Трансграничная передача персональных данных

5.5.1 Общество не осуществляет трансграничной передачи ПДн – передачи ПДн на территории иностранных государств, органам власти иностранных государств, иностранным физическим или юридическим лицам.

5.6 Сведения о третьих лицах, участвующих в обработке персональных данных

5.6.1 Общество вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено Федеральным законом, на основании заключаемого с этим лицом договора.

В договоре определяются:

- цели обработки ПДн;
- перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим их обработку;
- требования к защите обрабатываемых ПДн;
- обязательства об обеспечении конфиденциальности и безопасности ПДн при их обработке.

5.6.2 Лицо, осуществляющее обработку ПДн по поручению Общества, не обязано получать согласие субъекта ПДн на обработку его персональных данных.

5.6.3 В случае, если Общество поручает обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет Общество. Лицо, осуществляющее обработку ПДн по поручению Общества, несет ответственность перед Обществом.

5.7 Требования к защите персональных данных

5.7.1 Общество, при обработке ПДн, обеспечивает принятие необходимых правовых, организационных и технических мер защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения и иных неправомерных действий.

5.7.2 Обеспечение безопасности ПДн достигается:

- назначением лиц, ответственных за организацию обработки и обеспечение безопасности ПДн;
- изданием локальных нормативных актов, регламентирующих обработку и защиту ПДн, направленных на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

- определением перечня подразделений и должностей работников, допущенных к работе с ПДн;
- организацией обучения, оказания методической помощи, ознакомлением под роспись работников, осуществляющих обработку ПДн, с фактом участия в обработке ПДн, а также с правилами обработки и защиты ПДн, установленных нормативными правовыми актами Российской Федерации и локальными нормативными актами Общества;
- ведением регистрации и учета действий, совершаемых с ПДн;
- учётом материальных носителей ПДн и контролем их обращения в целях исключения утраты, хищения, подмены, несанкционированного копирования или уничтожения;
- ведением учета обращений субъектов ПДн;
- ограничением передачи ПДн внутри Общества только лицам, допущенным к работе с ПДн, занимающих должности, включенные в перечень подразделений и должностей работников, допущенных к работе с ПДн;
- обработкой ПДн в границах охраняемой территории (контролируемой зоны), а также организацией физической защиты носителей ПДн, мест и средств их обработки;
- контролем доступа в помещения, определенных для обработки ПДн и/или хранения их материальных носителей;
- определением угроз безопасности ПДн при их обработке в ИС ПДн, применением систем защиты и установлением правил доступа к ПДн;
- обнаружением фактов несанкционированного доступа к ПДн и принятием соответствующих мер;
- составлением типовых форм для сбора ПДн таким образом, чтобы каждый из субъектов ПДн имел возможность ознакомиться со своими ПДн, не нарушая прав и законных интересов иных субъектов ПДн;
- составление типовых форм сбора ПДн таким образом, чтобы субъект ПДн имел возможность проставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации (при необходимости получения письменного согласия на обработку ПДн);
- обеспечением взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных;
- периодическим контролем соответствия принимаемых мер требованиям законодательства Российской Федерации о ПДн и принятым в его исполнение локальным нормативным актам Общества.

6. Ответственность за нарушение правил обработки персональных данных

6.1 Временный генеральный директор Общества определяет приоритетные направления деятельности в области обеспечения сохранности обрабатываемых ПДн, меры по реализации настоящей Политики, а также осуществляет общее руководство через делегирование полномочий заместителю генерального директора по режиму и безопасности.

6.2 Ответственность за поддержание настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы обработки ПДн в Обществе, лежит на ОКБ и ОРП.

6.3 Руководители всех уровней Общества несут прямую ответственность за реализацию Политики и соблюдение ее положений подчиненными работниками.

6.4 Работники Общества, участвующие в обработке ПДн, несут персональную ответственность за несоблюдение требований настоящей Политики.

Ответственность за нарушение требований настоящей Политики определяется в соответствии с действующим законодательством и организационно-распорядительными документами Общества.

7. Контроль обработки персональных данных

7.1 Общий контроль работы с ПДн в Обществе осуществляет заместитель генерального директора по режиму и безопасности.

7.2 Текущий контроль соблюдения требований настоящей Политики осуществляют ОКБ и ОРП в рамках установленных полномочий. Контроль осуществляется путем проведения мониторинга и иных контрольных мероприятий.

8. Внесение изменений и дополнений

8.1 Изменения и дополнения в настоящую Политику вносятся при наличии следующих оснований:

- изменения законодательства Российской Федерации, нормативных распорядительных документов Корпорации и Общества, регламентирующих обработку ПДн;

- изменения организационно – штатной структуры Общества, касающиеся структурных подразделений, задействованных в реализации настоящей Политики.

9. Заключительные положения

9.1 Общество, как Оператор персональных данных (оператор) осуществляет обработку ПДн на территории и информационных ресурсах, принадлежащих ему на праве собственности.

Полное наименование и реквизиты Общества:

акционерное общество «Научно – исследовательский институт автоматизированных систем и комплексов связи «Нептун» (ИНН 7801563590);

фактический и почтовый адрес: 199178, Россия, г. Санкт-Петербург, 7 линия В.О., д.80, корп.1, лит. А.;

тел.: (812) 327-09-72, факс: (812) 323-31-78, эл. почта: inform@niineptun.ru, сайт <http://niineptun.ru>.

9.2 Уполномоченный орган по защите прав субъектов ПДн - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Управление по защите прав субъектов ПДн.

Территориальный орган Роскомнадзора по Северо-Западному федеральному округу: 190000, г. Санкт-Петербург, улица Садовая, дом 14/52, тел.: (812) 678-95-26, факс: (812) 571-27-31, e-mail: rsockanc78@rkn.gov.ru, сайт: <http://78.rkn.gov.ru>.