ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
ЛЕНМОРНИИПРОЕКТ
по проектированию, изысканиям и научным исследованиям
в области морского транспорта

Межевой канал, д. 3, корп. 2, Санкт-Петербург, 198035, тел.: (812) 703 40 10, факс: (812) 703 49 70, E-mail. lmniip@lmniip.spb.ru, www.lenmor.ru

УТВЕРЖДАЮ
Генеральный директор
ОАО «ЛЕНМОРНИИПРОЕКТ»
_____ /
«15» апреля 2014г.

ПОЛОЖЕНИЕ
О ПОРЯДКЕ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

РЕДАКЦИЯ №: 1

Введен впервые

Дата введения:		«___» _____	**2014 г.**
Срок действия:	**до**	«___» _____	**20___г.**
Приказ по ОАО №_____	**от**	«___» _____	**20___г.**
Продление срока действия:	**до**	«___» _____	**20___г.**
Приказ по ОАО №_____	**от**	«___» _____	**20___г.**

УЧЕТНЫЙ ЭКЗЕМПЛЯР №: 1

САНКТ-ПЕТЕРБУРГ

2014

РАЗРАБОТАНО:

Должность	Отдел	Фамилия, И. О.	Подпись	Дата
Руководитель	ЮО	Кондрашова Е.В.		

СОГЛАСОВАНО:

Должность	Отдел	Фамилия, И. О.	Подпись	Дата
Заместитель генерального директора по экономике и финансам	РУК	Рогач О.Г.		15.04.14
Заместитель генерального директора по информационным технологиям	РУК	Яковенко М.В.		15.04.14
Главный бухгалтер	РУК	Богданова Е.В.		
Руководитель	ОУП	Григорьева Е.С.		

1. Общие положения

1.1. Настоящее положение (далее - Положение) разработано в соответствии со ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" (далее - Закон о ПДн) и является основополагающим внутренним регулятивным документом открытого акционерного общества «*ЛЕНМОРНИИПРОЕКТ*» по проектированию, изысканиям и научным исследованиям в области морского транспорта (далее – Общество, Работодатель), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является Общество.

1.2. Положение разработано в целях реализации требований законодательства в области обработки и защиты ПДн и направлено на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Обществе, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайн.

1.3. Положение распространяются на отношения по обработке и защите ПДн, полученных Обществом как до, так и после утверждения Положения, за исключением случаев, когда по причинам правового, организационного и иного характера нормы Положения не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Если в отношениях с Обществом участвуют наследники (правопреемники) и (или) представители субъектов ПДн, то Общество становится оператором ПДн лиц, представляющих указанных субъектов. Положение и другие локальные нормативные акты Общества распространяются на случаи обработки и защиты ПДн наследников (правопреемников) и (или) представителей субъектов ПДн, даже если эти лица во внутренних регулятивных документах прямо не упоминаются, но фактически участвуют в правоотношениях с Обществом.

1.5. Действие настоящего Положения не распространяется на общедоступные источники персональных данных, в том числе справочники, адресные книги ОАО «*ЛЕНМОРНИИПРОЕКТ*», справки в составе тендерной документации, подготавливаемой в целях участия в конкурсах, аукционах. Перечень ПДн, которые могут содержаться в общедоступных источниках персональных данных, утверждается приказом Генерального директора.

2. Основания обработки, порядок получения и состав персональных данных, обрабатываемых в Обществе

2.1. Обработка ПДн в Обществе осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Общество выступает в качестве работодателя (гл. 14 Трудового кодекса Российской Федерации), в связи с реализацией Обществом своих прав и обязанностей как юридического лица, а также при взаимодействии с членами Совета директоров Общества.

2.2. В связи с трудовыми и иными непосредственно связанными с ними отношениями, в которых Общество выступает в качестве работодателя, обрабатываются ПДн лиц, претендующих на трудоустройство в Общество, работников Общества (далее - Работники) и бывших Работников.

2.3. В связи с реализацией своих прав и обязанностей, Обществом обрабатываются ПДн физических лиц, являющихся контрагентами Общества по гражданско-правовым договорам, физических лиц, ПДн которых используются для осуществления пропускного режима в здании Общества, а также акционеров – физических лиц, письменно обращающихся в Общество по вопросам его деятельности.

2.4. В рамках взаимодействия с членами Совета директоров Общества ПДн обрабатываются в ходе формирования данного органа управления Обществом.

2.5. Специальные категории персональных данных, а также биометрические персональные данные Обществом не обрабатываются.

2.6. ПДн получаются и обрабатываются Обществом на основании федеральных законов, а в необходимых случаях - при наличии письменного согласия субъекта ПДн.

2.7. Общество предоставляет обрабатываемые им ПДн государственным органам и организациям, имеющим, в соответствии с федеральным законом, право на получение соответствующих ПДн.

2.8. В Обществе не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Обществе, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Обществом ПНд уничтожатся или обезличиваются.

2.9. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. Общество принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

2.10. ПДн работника уполномоченное лицо Общества получает непосредственно от работника. Работодатель вправе получать персональные данные работника от третьих лиц только при наличии письменного согласия работника или в иных случаях, прямо предусмотренных в законодательстве РФ.

2.11. При изменении персональных данных работник письменно уведомляет Работодателя о таких изменениях в разумный срок, не превышающий 5 рабочих дней дней.

2.12. По мере необходимости Работодатель истребует у работника дополнительные сведения. Работник представляет требуемые сведения и в случае необходимости предъявляет документы, подтверждающие достоверность этих сведений

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в Обществе является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн Общество руководствуется следующими принципами:

1) законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

2) системность: обработка ПДн в Обществе осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

3) комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Общества (далее - ИС) и других имеющихся в Обществе систем и средств защиты;

4) непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

5) своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

6) преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Обществе с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере

защиты информации;

7) персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

8) минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

9) научная обоснованность и техническая реализуемость: уровень мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;

10) специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;

11) эффективность процедур отбора кадров и выбора контрагентов: кадровая политика Общества предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах Общества до заключения договоров;

12) наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

13) непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются;

14) достоверность сведений: при принятии решений, затрагивающих интересы работника, Работодатель не имеет права основываться на ПДн работника, полученных исключительно в результате их автоматизированной обработки или электронного поступления. Работодатель также не вправе принимать решения, затрагивающие интересы работника, основываясь на ПДн, допускающие двоякое толкование. В случае если на основании ПДн работника невозможно достоверно установить какой-либо факт, Работодатель предлагает работнику представить письменные разъяснения.

4. Доступ к обрабатываемым персональным данным

4.1. Доступ к обрабатываемым в Обществе ПДн имеют лица, уполномоченные приказом Общества, а также лица, чьи ПДн подлежат обработке.

4.2. В целях разграничения полномочий при обработке ПДн полномочия по реализации каждой функции (цели) Общества закрепляются за соответствующими структурными подразделениями Общества.

Доступ к ПДн, обрабатываемым в ходе реализации полномочий, закрепленных за конкретным структурным подразделением Общества, могут иметь только Работники этого структурного подразделения. Работники допускаются к ПДн, связанным с деятельностью другого структурного подразделения, только для чтения и подготовки обобщенных материалов в части вопросов, касающихся структурного подразделения этих Работников.

4.3. Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Общества.

Допущенные к обработке ПДн Работники под роспись знакомятся с документами Общества, устанавливающими порядок обработки ПНд, включая документы, устанавливающие права и обязанности конкретных Работников.

5. Реализация Положения

5.1. Общество принимает необходимые и достаточные меры для защиты обрабатываемых ПДн от неправомерного или случайного доступа к ним, от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц.

5.2. Ответственность за организацию обработки ПДн в Обществе несет руководитель отдела управления персоналом в соответствии с приказом Генерального директора Общества.

Ответственный за организацию обработки ПДн в Обществе, в частности, обязан:

1) осуществлять внутренний контроль за соблюдением в Обществе требований нормативных правовых актов и локальных нормативных актов Общества в области обработки и защиты ПДн;

2) доводить до сведения Работников положения нормативных правовых актов и локальных нормативных актов Общества в области обработки и защиты ПДн;

3) организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

5.3. Общество осуществляет обработку ПДн без использования средств автоматизации, а также с использованием таких средств.

5.4. При обработке ПДн без использования средств автоматизации Общество, в соответствии с положениями нормативных правовых актов в области обработки и защиты ПДн, реализует комплекс организационных и технических мер, обеспечивающих:

1) обособление ПДн от информации, не содержащей ПДн;

2) раздельную обработку и хранение каждой категории ПДн (фиксация на отдельных материальных носителях ПДн, цели обработки которых заведомо несовместимы);

3) соответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, установленным требованиям;

4) соблюдение установленных требований при ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн в здание Общества, или в иных аналогичных целях;

5) сохранность материальных носителей ПДн;

6) условия хранения, исключающие несанкционированный доступ к ПДн, а также смешение ПДн (материальных носителей), обработка которых осуществляется в различных целях;

7) надлежащее уточнение, уничтожение или обезличивание ПДн.

5.5. В соответствии с требованиями нормативных правовых актов в области обработки и защиты ПДн обработки ПДн с использованием средств автоматизации в Обществе создаются информационные системы персональных данных Общества (далее – ИСПДн).

Для каждой ИСПДн проводятся мероприятия по обеспечению безопасности информации в соответствии с требованиями законодательства.

Пересмотр моделей угроз для каждой ИСПДн осуществляется:

а) в плановом порядке для существующих ИСПДн - ежегодно;

б) в случае существенных изменений в инфраструктуре или порядке обработки ПДн в ИСПДн - в течение трех месяцев с даты фиксации изменений;

в) в случае создания новой ИСПДн (выделения части из существующей ИСПДн) - в течение одного месяца с даты создания (выделения) ИСПДн.

5.6. Обработка ПДн в Обществе с использованием средств автоматизации ведется только в ИСПДн. В Обществе запрещается обработка ПДн с целями, не соответствующими целям создания ИСПДн, эксплуатация ИСПДн в составе, отличном от указанного при создании ИСПДн.

5.7. Ввод в эксплуатацию ИСПДн оформляется актом ввода в эксплуатацию и ИСПДн.

5.8. Защита персональных данных реализуется комплексом правовых, режимных, организационных и программно-технических мер, которые включают:

1) подготовку локальных нормативных актов Общества по вопросам обработки и защиты ПДн, контроль за исполнением в Обществе требований нормативных правовых актов и локальных нормативных актов Общества в области обработки и защиты ПДн, а также внесение соответствующих изменений в имеющиеся внутренние регулятивные документы;

2) оформление письменных обязательств Работников о неразглашении ПДн;

3) доведение до сведения Работников информации об установленных законодательством Российской Федерации санкциях за нарушения, связанные с обработкой и защитой ПДн;

4) обеспечение наличия в положениях о структурных подразделениях Общества и должностных обязанностях Работников требований по соблюдению установленного порядка обработки и защиты ПДн;

5) разработку и введение в действие внутренних регулятивных документов Общества по обеспечению информационной безопасности ИСПДн;

6) ознакомление Работников с положениями нормативных правовых актов и локальных нормативных актов Общества в области обработки и защиты ПДн, а также обучение Работников правилам обработки и защиты ПДн;

7) проведение мероприятий по регламентации, установлению, поддержанию и осуществлению контроля за состоянием:

а) физической охраны, контрольно-пропускного режима, перемещением технических средств и носителей информации;

б) защиты технологических процессов, информационных ресурсов, информации и поддерживающей их инфраструктуры от угроз техногенного характера и внешних неинформационных воздействий;

8) регламентацию обработки ПДн, в том числе хранения и передачи информации как внутри Общества, так и при взаимодействии с контрагентами Общества, государственными органами и организациями, обращения с документами (включая электронные документы) и носителями, порядка их учета, хранения и уничтожения;

9) установление правил доступа на объекты, в помещения, в ИС, применению в этих целях систем охраны и управления доступом;

10) организацию технического оснащения объектов и ИСПДн в соответствии с существующими требованиями к информационной безопасности;

11) формирование условий и технологических процессов обработки, хранения и передачи информации в Обществе (включая условия хранения документов в архивах), обеспечивающих реализацию требований нормативных правовых актов, методических документов уполномоченных государственных органов и внутренних регулятивных документов Агентства в области обработки и защиты ПДн;

12) установление полномочий пользователей и форм представления информации пользователям ИСПДн;

13) организацию непрерывного процесса контроля (мониторинга) событий безопасности для своевременного выявления и пресечения попыток несанкционированного доступа к защищаемой информации;

14) организацию необходимых мероприятий с Работниками, а также собеседование с лицами, претендующими на работу в Обществе, изучение их биографии и проверку предоставляемых сведений; обучение Работников требованиям информационной безопасности;

15) осуществление контроля эффективности организационных мер защиты;

16) разработку защитных технических решений:

а) при стратегическом планировании архитектуры ИС;

б) выборе технических средств обработки информации;

в) разработке и (или) приобретении программного обеспечения;

6. Основные мероприятия по обеспечению безопасности персональных данных

6.1. Мероприятия по защите ПДн реализуются в Обществе в следующих направлениях:

1) предотвращение утечки информации, содержащей ПДн, по техническим каналам связи и иными способами;

2) предотвращение несанкционированного доступа к содержащей ПДн информации, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;

3) защита от вредоносных программ;

4) анализ защищенности ИСПДн;

5) обнаружение вторжений и компьютерных атак;

6) осуществления контроля за реализацией системы защиты ПДн.

6.2. Мероприятия по обеспечению безопасности ПДн включают в себя:

1) реализацию разрешительной системы допуска пользователей (Работников) к информационным ресурсам ИС и связанным с их использованием работам, документам;

2) разграничение доступа пользователей ИСПДн и обслуживающих ИСПДн Работников к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

3) предотвращение внедрения в ИС вредоносных программ и программных закладок, анализ принимаемой по информационно-телекоммуникационным сетям (сетям связи общего пользования) информации, в том числе на наличие компьютерных вирусов;

4) ограничение доступа в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации, содержащие ПДн;

5) размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

6) организацию физической защиты помещений и технических средств, позволяющих осуществлять обработку ПДн;

7) резервирование технических средств, дублирование массивов и носителей информации;

8) обнаружение вторжений в ИС, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

9) централизованное управление системой защиты ПДн в ИС.

6.3. С целью поддержания состояния защиты ПДн на надлежащем уровне в Обществе осуществляется внутренний контроль за эффективностью системы защиты ПДн и соответствием порядка и условий обработки и защиты ПДн установленным требованиям.

Внутренний контроль включает:

1) мониторинг состояния технических и программных средств, входящих в состав СЗПДн;

2) контроль соблюдения требований по обеспечению безопасности ПДн (требований нормативных правовых актов и локальных нормативных актов в области обработки и защиты ПДн, требований договоров).

6.4. В целях осуществления внутреннего контроля в Обществе проводятся периодические проверки условий обработки ПДн. Такие проверки осуществляются ответственным за организацию обработки ПДн в Обществе либо комиссией, образуемой и

назначаемой в соответствии с приказом Генерального директора Общества.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывается Генеральному директору Общества.