АО «ДАЛЬГИПРОТРАНС»

АКЦИОНЕРНОЕ ОБЩЕСТВО
«ДАЛЬНЕВОСТОЧНЫЙ ПРОЕКТНО-ИЗЫСКАТЕЛЬСКИЙ
ИНСТИТУТ ТРАНСПОРТНОГО СТРОИТЕЛЬСТВА»

СТАНДАРТ ОРГАНИЗАЦИИ

ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
В АО ДАЛЬГИПРОТРАНС

СТО-28.02-2021

Хабаровск
2021

УТВЕРЖДАЮ
Генеральный директор
АО «Дальгипротранс»
_____ А.В. Лобов
«07» октября 2021 год

СТАНДАРТ ОРГАНИЗАЦИИ

ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
В АО ДАЛЬГИПРОТРАНС

СТО-28.02-2021

Документ введен: приказом № 197а от «07» октября 2021 г.

Введен взамен СТП-П-11.2-2011

Дата введения: «07» октября 2021 г.

Содержание

ВВЕДЕНИЕ....3
1 ОБЛАСТЬ ПРИМЕНЕНИЯ И СФЕРА ДЕЙСТВИЯ....3
2 НОРМАТИВНЫЕ ССЫЛКИ....3
3 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ....4
4 ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ....6
5 ОБЩИЕ ПОЛОЖЕНИЯ....6
6 ОСНОВНЫЕ ПРАВА И ОБЯЗАННОСТИ ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ....7
7 ОСНОВНЫЕ ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ....7
8 ЦЕЛИ СБОРА И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ....8
9 ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ....8
10 КАТЕГОРИИ СУБЪЕКТОВ И ОБЪЕМ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ....9
11 ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ....11
12 ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ....12
13 ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ (НЕАВТОМАТИЗИРОВАННАЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ)....12
14 ОРГАНИЗАЦИЯ ОБРАБОТКИ ОБРАЩЕНИЙ И ЗАПРОСОВ....14
15 ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ....16
16 УПРАВЛЕНИЕ ЗАПИСЯМИ....19
17 ОТВЕТСТВЕННОСТЬ....19
Приложение 1 Форма отчета о результатах проведения проверки....20

ВВЕДЕНИЕ

Настоящая Политика в отношении обработки персональных данных в АО «Дальгипротранс» (далее – Политика) разработана во исполнение требований п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Политика является основополагающим документом, определяющим общие принципы, цели, способы, объем и порядок обработки персональных данных в АО «Дальгипротранс» (далее – Общество, Оператор), а также общую стратегию построения системы защиты персональных данных при их обработке.

1 ОБЛАСТЬ ПРИМЕНЕНИЯ И СФЕРА ДЕЙСТВИЯ

1.1 Требования настоящей Политики распространяются на всех работников Общества (штатных, временных, работающих по контракту и т.п.), кандидатов на замещение вакантных должностей, лиц, находящихся в кадровом резерве, а также всех прочих лиц (арендаторы, контрагенты, посетители и т.п.) при необходимости их участия в процессе обработки персональных данных Оператором.

1.2 Настоящая Политика распространяется на все структурные подразделения Общества.

1.3 Политика действует в отношении всех персональных данных, обрабатываемые Оператором, которые необходимы в соответствии с определяемыми настоящей Политикой целями сбора и обработки персональных данных.

1.4 Политика распространяется на отношения в области обработки персональных данных, возникшие у Оператора как до, так и после утверждения настоящей Политики, до ее замены новой версией.

1.5 Во исполнение требований ч. 2 ст. 18.1 Закона о персональных данных настоящая Политика в целях обеспечения неограниченного доступа к документу размещается на информационном стенде Общества и (или) публикуется в свободном доступе в информационно-телекоммуникационной сети Интернет на сайте Общества.

2 НОРМАТИВНЫЕ ССЫЛКИ

В настоящей Политике использованы следующие документы:

2.1 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

2.2 Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

2.3 Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

2.4 Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

2.5 Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

2.6 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».

3 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

3.1 Для целей настоящей Политики используются следующие основные понятия:

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

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

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закон о персональных данных - Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с федеральными законами, иными нормативными актами Российской Федерации, или требованиями, устанавливаемыми собственником информации.

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

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

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.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность персональных данных - операторы и иные лица, получившие

доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, осуществляемая при непосредственном участии человека без использования средств вычислительной техники.

Недекларированные возможности средств вычислительной техники – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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;

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.

Общество / Оператор персональных данных – Акционерное Общество «Дальневосточный проектно-изыскательный институт транспортного строительства» (АО «Дальгипротранс»).

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.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных .

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

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система защиты персональных данных – совокупность организационных и технических мер по обеспечению безопасности персональных данных при их обработке.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

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

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

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.

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.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость информационной системы – недостатки или некая слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

4 ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящей Политике не применяются какие-либо сокращения.

5 ОБЩИЕ ПОЛОЖЕНИЯ

5.1 Целью настоящей Политики является создание в Обществе единой системы взглядов и понимания целей, принципов и порядка обработки персональных данных, защита прав субъектов персональных данных при их обработке.

5.2 Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает Оператор.

Меры по обеспечению безопасности персональных данных реализуются в Обществе в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября

2012 г. № 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

5.3 Контроль за исполнением требований настоящей Политики осуществляется уполномоченным лицом, ответственным за организацию обработки персональных данных у Оператора.

Лицо, ответственное за организацию обработки персональных данных, назначается приказом руководителя Общества.

В обязанности лица, ответственного за организацию обработки персональных данных, входит:

1) осуществление внутреннего контроля за соблюдением Оператором и работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доведение до сведения работников Оператора положения законодательства Российской Федерации о персональных данных, локальных нормативных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов.

6 ОСНОВНЫЕ ПРАВА И ОБЯЗАННОСТИ ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1 При обработке персональных данных Оператор обязан:

1) организовывать обработку персональных данных в соответствии с требованиями Закона о персональных данных;

2) отвечать на обращения и запросы субъектов персональных данных и их законных представителей в соответствии с требованиями Закона о персональных данных;

3) сообщать в уполномоченный орган по защите прав субъектов персональных данных (Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)) по запросу этого органа необходимую информацию в течение 30 дней с даты получения такого запроса;

4) прекратить по требованию субъекта персональных данных обработку его персональных данных в случаях и порядке, установленными Законом о персональных данных.

6.2 Оператор имеет право:

1) самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Законом о персональных данных или другими федеральными законами;

2) поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных;

3) в случае отзыва субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Законе о персональных данных.

7 ОСНОВНЫЕ ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1 Субъект персональных данных имеет право:

1) получать информацию, касающуюся обработки его персональных данных, за исключением случаев, предусмотренных федеральными законами. Сведения предоставляются субъекту персональных данных Оператором в доступной форме, и в них не должны

содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных. Перечень информации и порядок ее получения установлен Законом о персональных данных;

2) требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

3) обжаловать в Роскомнадзоре или в судебном порядке неправомерные действия или бездействие Оператора при обработке его персональных данных.

8 ЦЕЛИ СБОРА И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1 Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

8.2 Обработке подлежат только персональные данные, которые отвечают целям их обработки.

8.3 Обработка Оператором персональных данных осуществляется в следующих целях:

- регулирования трудовых отношений с работниками Общества (трудоустройство, ведение кадрового делопроизводства, обучение);
- привлечения и отбора кандидатов на работу у Оператора;
- исполнения обязанностей, возложенных законодательством Российской Федерации на Оператора, в том числе связанные с предоставлением персональных данных в налоговые органы, Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования, а также в иные государственные органы;
- предоставления работникам Общества и членам их семей дополнительных гарантий и компенсаций, в том числе добровольного медицинского страхования, негосударственного пенсионного обеспечения и других видов социального обеспечения;
- подготовки, заключения, исполнения и прекращения договоров с контрагентами;
- осуществления пропускного режима;
- исполнения судебных актов, актов других государственных органов или должностных лиц;
- реализации прав и законных интересов Общества в рамках ведения видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Общества, или третьих лиц либо достижения общественно значимых целей, при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- в иных целях, установленных федеральными законами, иными нормативными правовыми актами Российской Федерации.

9 ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1 Правовым основанием обработки персональных данных является совокупность нормативных актов Российской Федерации, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных, в том числе:

- Конституция Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах»;
- Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;
- Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном

страховании в Российской Федерации»;

- иные нормативные акты Российской Федерации, регулирующие отношения, связанные с деятельностью Оператора.

9.2 Правовым основанием обработки персональных данных также являются:

- устав АО «Дальгипротранс»;
- Коллективный договор АО «Дальгипротранс» (с учетом дополнительных соглашений);
- договоры, заключаемые между Оператором и субъектами персональных данных;
- согласие субъектов персональных данных на обработку их персональных данных.

10 КАТЕГОРИИ СУБЪЕКТОВ И ОБЪЕМ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1 Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, предусмотренным в Разделе 8 настоящей Политики. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

10.2 Оператор может обрабатывать персональные данные следующих категорий субъектов персональных данных.

10.2.1 Кандидаты на замещение вакантных должностей Оператора:

- фамилия, имя, отчество;
- пол;
- гражданство;
- дата и место рождения;
- контактные данные;
- сведения об образовании, опыте работы, квалификации;
- иные персональные данные, сообщаемые кандидатами в резюме и сопроводительных письмах.

10.2.2. Работники Оператора (в том числе бывшие):

- фамилия, имя, отчество;
- пол;
- гражданство;
- дата и место рождения;
- изображение (фотография);
- паспортные данные;
- адрес регистрации по месту жительства;
- адрес фактического проживания;
- контактные данные;
- индивидуальный номер налогоплательщика;
- страховой номер индивидуального лицевого счета (СНИЛС);
- сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации;
- семейное положение, наличие детей;
- сведения о трудовой деятельности;
- данные о регистрации брака;
- сведения о воинском учете;
- сведения об инвалидности;
- сведения об удержании алиментов;
- сведения о доходе с предыдущего места работы;
- иные персональные данные, предоставляемые работниками в соответствии с федеральными законами, иными нормативными актами Российской Федерации.

10.2.3 Члены семьи работников Оператора:

- фамилия, имя, отчество;
- степень родства;
- дата рождения;
- иные персональные данные, предоставляемые работниками в соответствии с федеральными законами, иными нормативными актами Российской Федерации.

10.2.4 Стажеры и практиканты Оператора:

- фамилия, имя, отчество;
- пол;
- гражданство;
- дата и место рождения;
- контактные данные;
- сведения об образовании, опыте работы, квалификации;
- иные персональные данные, в соответствии с федеральными законами, иными нормативными актами Российской Федерации.

10.2.5 Контрагенты Оператора (физические лица):

- фамилия, имя, отчество;
- дата и место рождения;
- паспортные данные;
- адрес регистрации по месту жительства;
- контактные данные;
- индивидуальный номер налогоплательщика;
- номер расчетного счета;
- иные персональные данные, предоставляемые контрагентами (физическими лицами), необходимые для заключения и исполнения договоров.

10.2.6 Представители (работники) контрагентов Оператора (юридических лиц):

- фамилия, имя, отчество;
- паспортные данные;
- контактные данные;
- замещаемая должность;
- иные персональные данные, предоставляемые представителями (работниками) контрагентов, необходимые для заключения и исполнения договоров.

10.2.7 Посетители Оператора:

- фамилия, имя, отчество;
- паспортные данные;
- сведения о трудовой деятельности (место работы);
- иные персональные данные, предоставляемые посетителями в соответствии с Положением о пропускном и внутриобъектовом режимах.

10.2.8 Лица, входящие в органы управления Общества и ревизионную комиссию в соответствии с Уставом Общества:

- фамилия, имя, отчество;
- гражданство;
- дата и место рождения;
- паспортные данные;
- адрес регистрации по месту жительства;
- контактные данные;
- индивидуальный номер налогоплательщика;
- страховой номер индивидуального лицевого счета (СНИЛС);
- иные персональные данные, предоставляемые в соответствии с федеральными законами, иными нормативными актами Российской Федерации.

10.3 Обработка Оператором биометрических персональных данных (сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность) осуществляется в соответствии с федеральными законами,

иными нормативными актами Российской Федерации и локальными нормативными актами Общества.

10.4 Оператором не осуществляется обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, если это предусмотрено федеральными законами, иными нормативными актами Российской Федерации.

11 ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1 Обработка персональных данных осуществляется в Обществе с соблюдением требований федеральных законов и иных нормативных актов Российской Федерации в соответствии с утверждаемым приказом руководителя Общества Положением о персональных данных.

11.2 Обработка персональных данных осуществляется с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных федеральными законами и иными нормативными актами Российской Федерации.

11.3 К обработке персональных данных допускаются работники Оператора, в должностные обязанности которых входит обработка персональных данных.

11.4 Обработка персональных данных осуществляется путем:

- получения персональных данных в устной и письменной форме непосредственно от субъектов персональных данных;
- получения персональных данных из общедоступных источников;
- внесения персональных данных в журналы, реестры и информационные системы персональных данных Оператора, хранение персональных данных;
- предоставление персональных данных в налоговые органы, Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования, в иные государственные органы, а также в случаях выдачи доверенности на право представления интересов Общества;
- использования иных способов обработки персональных данных, предусмотренных настоящей Политикой, федеральными законами и иными нормативными актами Российской Федерации.

11.5 Не допускается предоставление третьим лицам или распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральными законами и иными нормативными актами Российской Федерации.

11.6 Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Пенсионный фонд Российской Федерации, Фонд социального страхования и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с федеральными законами и иными нормативными актами Российской Федерации.

11.7 Оператор принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, распространения и других несанкционированных действий.

11.8 Оператор осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральными законами, иными нормативными актами Российской Федерации, договором с субъектом персональных данных.

11.9 При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

12 ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

12.1 Обработка персональных данных в информационных системах персональных данных в Обществе осуществляется в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

12.2 Общество организует режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, а также режим обеспечения сохранности носителей персональных данных.

12.3 Руководитель Общества утверждает перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.

12.4 Пользователем информационной системы персональных данных в Обществе является работник Общества, имеющий доступ к информационной системе персональных данных и ее ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями.

Все работники Общества, являющиеся пользователями информационной системы персональных данных, должны быть ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными нормативными актами по вопросам обработки персональных данных и выполнять установленные в них правила по соблюдению принятого режима безопасности персональных данных.

12.5 Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

12.6 Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Общества, третьим лицам.

12.7 При работе с персональными данными в информационной системе работники Общества обязаны обеспечить отсутствие возможности доступа к информационной системе третьих лиц, а также просмотра персональных данных третьими лицами с мониторов рабочих мест.

12.8 При завершении работы с информационной системой персональных данных работники обязаны защитить рабочее место с помощью блокировки паролем.

12.9 Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы информационной системой персональных данных, могущих повлечь за собой угрозы безопасности персональных данных, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, руководству структурного подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности персональных данных.

13 ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ (НЕАВТОМАТИЗИРОВАННАЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ)

13.1 Обработка персональных данных без использования средств автоматизации (неавтоматизированная) – это обработка персональных данных, в том числе содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных,

осуществляются при непосредственном участии человека и (или) без помощи средств вычислительной техники.

13.2 Обработка персональных данных без использования средств автоматизации в Обществе осуществляется в соответствии с Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

13.3 Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

13.4 При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

13.5 В Обществе обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

13.6 Фиксация персональных данных при неавтоматизированной обработке может осуществляться на бумажных и других материальных носителях, считывание информации с которых может производиться без использования средств вычислительной техники.

Персональные данные фиксируются на материальном носителе неавтоматизированным способом (например, записью "от руки" на листе бумаги) или автоматизированным способом (выводом на печать или копированием информации, содержащей персональные данные, на носитель с использованием средств вычислительной техники).

13.7 При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

13.8 Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данные, зафиксированных на материальном носителе (удаление, вымарывание).

13.9 Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

13.10 Бумажные носители и иные материальные носители, содержащие персональные данные, хранятся в сейфах, запираемых шкафах или ящиках столов, находящихся в помещениях подразделений Общества.

Материальные носители, содержащие персональные данные, обрабатываемые в различных целях, хранятся раздельно (в разных шкафах, на разных полках, в отдельных ящиках или папках и т.п.).

В рабочее время документы, содержащие персональные данные, не должны находиться на столах работников отделов дольше времени необходимого на их обработку. Во время обработки документы, содержащие персональные данные, по возможности размещаются таким образом, чтобы исключить возможность просмотра информации посторонними лицами.

В конце рабочего дня все документы, содержащие персональные данные, должны быть убраны в сейфы или шкафы, закрывающиеся на замок. Черновики и редакции документов, испорченные бланки, листы со служебными записями в конце рабочего дня уничтожаются механическим путём до состояния, не позволяющего считывать информацию с носителей.

Испорченные бланки, черновики и промежуточные редакции документов, содержащие персональные данные, по окончании работы с ними уничтожаются.

13.11 В целях организации пропускного и внутриобъектового режима в административно-производственных зданиях и на территории Общества ведутся журналы (реестры, книги), содержащие персональные данные, необходимые для однократного пропуска субъекта персональных данных на территории, на которых находятся структурные подразделения Общества. Для таких журналов (реестров, книг) должны соблюдаться следующие условия:

1) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

2) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

Необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных.

14 ОРГАНИЗАЦИЯ ОБРАБОТКИ ОБРАЩЕНИЙ И ЗАПРОСОВ

14.1 Субъект персональных данных или его законный представитель имеет право на получение от Оператора информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных

настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные Федеральным законом о персональных данных или другими федеральными законами.

Субъект персональных данных вправе отозвать свое согласие на обработку персональных данных и/или требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

14.2 Обработка обращений и запросов субъектов персональных данных или их представителей осуществляется отделом управления персоналом.

С целью регистрации обращений и запросов по вопросам обработки персональных данных, а также ответов на них, ведется в специальный журнал учета запросов и обращений по вопросам персональных данных.

14.3 Запрос (обращение) субъекта персональных данных должен содержать:

- фамилию, имя и отчество субъекта персональных данных;
- паспортные данные субъекта персональных данных (его представителя);
- сведения, подтверждающие участие субъекта персональных данных в отношениях с Обществом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных субъекта персональных данных Обществом;
- текст содержания запроса (обращения);
- адрес для получения ответа на запрос (обращение);
- подпись субъекта персональных данных (его представителя).

14.5 Отдел управления персоналом в целях формирования ответа на запрос (обращение) об обработке персональных данных субъектов персональных данных запрашивает и получает необходимую информацию в соответствующем структурном подразделении Общества, осуществляющем обработку персональных данных субъекта персональных данных. Структурные подразделения, в которых обрабатываются указанные в запросе (обращении) персональные данные, обеспечивают предоставление информации отделу управления персоналом в течение 3 (трех) рабочих дней.

14.6 При получении запроса на **уточнение** персональных данных необходимые изменения вносятся в срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, и отправляется уведомление о внесенных изменениях.

14.7 При получении запроса на **уничтожение** персональных данных персональные данные уничтожаются в срок, не превышающий 7 рабочих дней со дня представления субъектом персональных данных сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, и отправляется уведомление об уничтожении.

14.8 При получении запроса на **отзыв согласия** на обработку персональных данных такая обработка прекращается и, в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, персональные данные уничтожаются в срок, не превышающий 30 дней с даты поступления указанного отзыва.

14.9 При **выявлении недостоверности** персональных данных при обращении или по запросу субъекта персональных данных персональные данные блокируются с момента такого обращения или получения такого запроса на период проверки. Если факт недостоверности персональных данных подтвержден на основании сведений, представленных субъектом

персональных данных, персональные данные уточняются в течение 7 рабочих дней со дня представления таких сведений и снимается блокирование персональных данных. Если факт недостоверности персональных данных не подтвержден, субъекту персональных данных отправляется уведомление об отказе изменения персональных данных.

14.10 При выявлении **неправомерной обработки** персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки.

14.11 При выявлении неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

14.12 При выявлении неправомерной обработки персональных данных, осуществляемой оператором, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

14.13 При **достижении целей** обработки персональных данных такая обработка незамедлительно прекращается, соответствующие персональные данные уничтожаются в срок, не превышающий 30 дней с даты достижения цели обработки персональных данных.

14.14 В случае, если сведения, указанные в п.14.1, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в п.14.1 и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральными законами, иными нормативными актами.

Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в п.14.1., а также в целях ознакомления с обрабатываемыми персональными данными до истечения тридцатидневного срока, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п.14.3., должен содержать обоснование направления повторного запроса.

15 ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

15.1 Обеспечение безопасности персональных данных при их обработке в Обществе осуществляется в соответствии:

1) федеральными законами и нормативными актами Российской Федерации в области обработки и защиты персональных данных;

2) с требованиями ФСТЭК России, ФСБ России и Роскомнадзора;

3) с локальными нормативными актами Общества.

15.2 Система защиты персональных данных включает в себя комплекс организационных и (или) технических мер, обеспечивающих безопасность персональных данных, в том числе:

1) принятие локальных нормативных актов, регулирующих отношения в сфере обработки и защиты персональных данных;

2) назначение лиц, ответственных за обеспечение безопасности персональных данных в структурных подразделениях и информационных системах Оператора;

3) организацию работы с персональными данными, обеспечивающей сохранность носителей персональных данных и средств защиты информации;

4) разграничение доступа пользователей и работников, обслуживающих средства вычислительной техники, к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

5) размещение информационных систем, обрабатывающих персональные данные, и специального оборудования в помещениях, исключающих возможность неконтролируемого пребывания в них посторонних лиц;

6) определение угроз безопасности персональных данных при их обработке;

7) учет документов и информационных массивов, содержащих персональные данные;

8) регистрацию действий пользователей информационных систем, обрабатывающих персональные данные, и работников, обслуживающих средства вычислительной техники в установленном оператором порядке;

9) контроль действий и недопущение несанкционированного доступа к персональным данным пользователей информационных систем Общества и персонала, обслуживающего средства вычислительной техники;

10) хранение и использование материальных носителей персональных данных, в условиях, исключающих их хищение, подмену и уничтожение;

11) иные меры, обеспечивающие безопасность персональных данных при их обработке.

15.3 Для каждой информационной системы, обрабатывающей персональные данные, в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, в зависимости от уровня защищенности персональных данных при их обработке в информационных системах назначается должностное лицо (работник), ответственное за обеспечение безопасности персональных данных в информационной системе.

15.4 Организационные и (или) технические меры защиты для каждой информационной системы, обрабатывающей персональные данные, определяются с учетом уровней защищенности персональных данных, актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационной системе Общества.

Уровень защищенности информационных систем, обрабатывающих персональные данные, определяется в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных.

Содержание каждой из мер по обеспечению безопасности персональных данных, определено Приказом 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».

15.5 Выбор организационных и (или) технических мер защиты определяется Оператором самостоятельно.

15.6 В целях определения системы защиты для информационных систем, обрабатывающих персональные данные в Обществе, комиссией, назначаемой приказом руководителя Общества, проводится проверка на предмет выявления:

- информационных систем персональных данных, используемых в Обществе,
- перечня персональных данных, обрабатываемых в Обществе и подлежащих защите,

- групп пользователей, работающих с персональными данными в Обществе, уровне их доступа и информированности.

15.7 В целях определения системы защиты персональных данных при их обработке, осуществляемой без использования средств автоматизации в Обществе, комиссией, назначаемой приказом руководителя Общества, проводится проверка на предмет выявления:

• мест хранения материальных носителей персональных данных (с указанием номеров кабинетов);

• перечня персональных данных, обрабатываемых в Обществе и подлежащих защите;

• групп пользователей, работающих с персональными данными в Обществе, уровне их доступа и информированности.

15.8 Проверки, указанные в п. 15.6 и п. 15.7 настоящей Политики, проводятся ежегодно.

15.9 По результатам проверок лицо, ответственное за организацию обработки персональных данных, оформляет Отчет о результатах проведения проверки (Приложение 1).

В Отчете должны быть отражены в частности:

- выявленные в результате внутренней проверки информационные системы персональных данных, используемые в Обществе;
- выявленные места хранения материальных носителей персональных данных (с указанием номеров кабинетов);
- перечень персональных данных, обрабатываемых в Обществе и подлежащих защите;
- группы пользователей, работающих с персональными данными в Обществе, уровне их доступа и информированности;
- информация о разграничении прав доступа к обрабатываем персональным данным;
- выявленные угрозы безопасности персональных данных;
- перечень мероприятий, обеспечивающих защиту персональных данных.

15.10 Разработка мер и контроль над обеспечением безопасности персональных данных осуществляется лицом, ответственным за организацию обработки персональных данных.

Лицо, ответственное за организацию обработки персональных данных, ведет работу по следующим направлениям обеспечения безопасности персональных данных:

- планирование и реализация мер по обеспечению безопасности персональных данных;
- анализ угроз безопасности персональных данных;
- разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, регламентов, инструкций и других организационных документов по обеспечению безопасности;
- контроль защищенности ИТ-инфраструктуры Общества от угроз информационной безопасности;
- информирование пользователей персональных данных о порядке работы с персональными данными и средствами защиты;
- контроль исполнения требований по защите персональных данных в структурных подразделениях Общества;
- предотвращение, выявление, реагирование и расследование нарушений безопасности персональных данных.

16 УПРАВЛЕНИЕ ЗАПИСЯМИ

Наименование записи	Периодичность ведения записи	Лицо, ответственное за ведение записи	Подразделение, ответственное за хранение записи / срок хранения	Ссылка на приложение
1	2	3	4	5
Отчет о результатах проведения проверки	По результатам проведения проверок в соответствии с п. 15.6 и п 15.7 настоящей Политики	Лицо, ответственное за организацию обработки персональных данных, назначаемое приказом руководителя Общества	Хранится в отделе обеспечения безопасности / 5 лет	Приложение 1

17 ОТВЕТСТВЕННОСТЬ

17.1 Ответственность за нарушение требований федеральных законов, иных нормативных актов Российской Федерации и локальных нормативных актов Общества в сфере обработки и защиты персональных данных определяется в соответствии с законодательством Российской Федерации.

17.2 Лица, виновные в нарушении требований федеральных законов, иных нормативных актов Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к административной, гражданско-правовой или уголовной ответственности в порядке, установленном федеральными законами.

17.3 Моральный вред, причиненный работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, а также несоблюдения требований к защите персональных данных, установленных Законом о персональных данных, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных работником убытков.

Приложение 1

Форма отчета о результатах проведения проверки

ОТЧЕТ
о результатах проведения проверки

г. Хабаровск «___» _____ 20__ г.

Состав комиссии:
Председатель - Должность Фамилия И.О.
Члены комиссии - Должность Фамилия И.О.

Настоящий Отчет о результатах проведения проверки подготовлен по результатам внутренней проверки по выявлению информационных систем, обрабатывающих персональные данные в Обществе, и условий неавтоматизированной обработки персональных данных в АО «Дальгипротранс» во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) и преследует цель установления уровня защищенности персональных данных для определения существующих и необходимых мер защиты персональных данных.

ОБЩИЕ ПОЛОЖЕНИЯ

Внутренняя проверка (далее – Проверка) проведена на основании приказа №___ от ____.

Проверка проводилась в соответствии с положениями Политики в отношении обработки персональных данных в АО «Дальгипротранс».

I. ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

В целях определения системы защиты для информационных систем, обрабатывающих персональные данные в Обществе, комиссией проведена проверка на предмет выявления:

- информационных систем персональных данных, используемых в Обществе,
- перечня персональных данных, обрабатываемых в Обществе и подлежащих защите,
- групп пользователей, работающих с персональными данными в Обществе, уровне их доступа и информированности.

РЕЗУЛЬТАТЫ ПРОВЕРКИ

…..

МЕРЫ, НЕОБХОДИМЫЕ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНВЫХ ДАННЫХ

…..

II. НЕАВТОМАТИЗИРОВАННАЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

В целях определения системы защиты персональных данных при их обработке, осуществляемой без использования средств автоматизации в Обществе, комиссией проведена проверка на предмет выявления:

- мест хранения материальных носителей персональных данных (с указанием номеров кабинетов);
- перечня персональных данных, обрабатываемых в Обществе и подлежащих защите;
- групп пользователей, работающих с персональными данными в Обществе, уровне их доступа и информированности.

РЕЗУЛЬТАТЫ ПРОВЕРКИ

…..

МЕРЫ, НЕОБХОДИМЫЕ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНВЫХ ДАННЫХ

…..

Подписи:

ЛИСТ СОГЛАСОВАНИЙ

РАЗРАБОТАЛ

Должность	ФИО	Дата	Подпись
Ведущий специалист отдела обеспечения безопасности	Бурнина-Пассар Л.Е.	11.08.2021	

ПРОВЕРИЛ

Должность	ФИО	Дата	Подпись
Инженер 1 категории отдела технического регулирования и инноваций	Боброва Д.А.	11.08.2021	

СОГЛАСОВАНО

Должность	ФИО	Дата	Подпись
Главный инженер	Трубников Е.А.	30.09.2021	
Заместитель генерального директора по экономической безопасности	Коротчук Г.И.	12.08.2021	
Начальник отдела управления персоналом	Ховрина О.Н.	12.08.2021	
Начальник отдела информационных технологий	Вершинин А.В.	13.08.2021	
Начальник юридического отдела	Замараева Е.В.	24.09.2021	
Начальник отдела технического регулирования и инноваций	Бадяев И.В.	16.08.2021	