Приложение № 2
к Приказу № 9/1/1 от «26» мая 2022 г.

УТВЕРЖДАЮ
Генеральный директор
ООО «Орион Экспресс»

_____ К.И. Махновский

«26» мая 2022 г.

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
в ООО «Орион Экспресс»

г. Москва 2022

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение «О защите персональных данных» (далее – Положение) обеспечивает защиту прав и свобод человека и гражданина при обработке его персональных данных, а также устанавливает общие требования к обеспечению безопасности персональных данных, обрабатываемых в ООО «Орион Экспресс» (далее – Компания).

1.2. Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информатизации, информационных технологиях и о защите информации», Постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Распоряжением Правительства РФ от 21.03.1994 № 358-р «Об обеспечении сохранности документов по личному составу», Приказом ФСТЭК России от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер при обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и иными нормативными актами, действующими на территории Российской Федерации

1.3. В настоящем Положении используются следующие термины и определения:

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

Обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу (в том числе распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор персональных данных - 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.

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

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

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

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

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения или предоставления третьим лицам без согласия субъекта персональных данных или требования Федерального закона.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по функциональным и техническим характеристикам.

Работник – физическое лицо, вступившее в трудовые отношения с Компанией.

1.4. Настоящее Положение вступает в силу со дня его утверждения Генеральным Директором.

1.5. Настоящее Положение распространяется на все Персональные данные, обрабатываемые Компанией, и обязательно для применения всеми Работниками Компании, осуществляющими обработку Персональных данных в силу своих должностных обязанностей.

1.6. Настоящее Положение доводится до сведения всех Работников персонально под роспись.

II. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных в Компании осуществляется при соблюдении следующих условий:

2.1.1. персональные данные обрабатываются исключительно в объеме, требуемом для достижения целей их обработки;

2.1.2. принятие необходимых технических и организационных мер по защите персональных данных;

2.1.3. персональные данные носят конфиденциальный характер. Работники Компании, имеющие доступ к персональным данным в силу своих должностных обязанностей, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством РФ;

2.1.4. срок обработки персональных данных не должен превышать сроков, необходимых для достижения целей обработки персональных данных, а также сроков хранения персональных данных, определенных действующим законодательством РФ;

2.1.5. использование Компанией баз данных, находящихся на территории РФ, при обработке и хранении персональных данных.

2.2. Все персональные данные субъекта следует получать у него самого, за исключением случаев, если в силу закона их получение возможно у третьей стороны.

2.3. Компания не имеет права получать и обрабатывать сведения о субъектах персональных данных, отнесенные законодательством РФ к специальной категории персональных данных, за исключением случаев, предусмотренных законодательством РФ.

2.4. Компания вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено законодательством РФ. В случае, если Компания на основании договора поручает обработку персональных данных другому лицу, существенным условием такого договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке. Кроме того в поручении на обработку персональных данных должны быть определены перечень действий с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели их обработки.

2.5. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если иной срок хранения персональных данных не установлен законодательством РФ.

2.6. Хранение персональных данных осуществляется:

- в электронном виде (на серверах, а также на внешних цифровых носителях – в специально оборудованных шкафах и сейфах);

- на бумажных носителях, в специально оборудованных шкафах и сейфах.

2.7. При хранении персональных данных на материальных носителях не допускается сохранение на одном материальном носителе персональных данных, цели обработки которых отличаются.

2.8. Серверы базы данных Компании расположены на территории РФ по адресу: 123308, г. Москва, ул. Демьяна Бедного, д.24, корпус 1.

III. МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обеспечение конфиденциальности и безопасности персональных данных в ИСПДн достигается посредством комплекса правовых, организационных и технических мер, направленных на предотвращение несанкционированного доступа к ним, уничтожения, блокирования, копирования, распространения персональных данных субъектов, а также иных неправомерных действий.

3.2. Организационные меры, направленные на обеспечение конфиденциальности и безопасности персональных данных и их обработки, предусматривают:

3.2.1. разработку и утверждение локальных нормативных актов Компании, регламентирующих вопросы обработки и защиты персональных данных и отвечающих требованиям нормативных правовых актов РФ;

3.2.2. организация режима обеспечения безопасности помещений Компании, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

3.2.3. утверждение перечня лиц, имеющих доступ к персональным данным для выполнения ими служебных обязанностей;

3.2.4. получение согласий на обработку персональных данных у субъектов персональных данных;

3.2.5. учет технических средств ИСПДн Компании, в том числе носителей персональных данных. Лицам, допущенным к обработке персональных данных, запрещается использовать сторонние технические и программные средства, не входящие в состав ИСПДн Компании;

3.2.6. организация мероприятий по обеспечению сохранности носителей персональных данных в соответствии с Инструкцией по работе с носителями персональных данных;

3.2.7. ознакомление работников с правилами обработки и защиты персональных данных;

3.2.8. определение ответственного за обеспечение безопасности обработки и защиты персональных данных;

3.2.9. организация деятельности по работе с обращениями и запросами субъектов персональных данных.

3.3. Технические меры по обеспечению безопасности персональных данных при их обработке в ИСПДн Компании устанавливаются с учетом:

3.3.1. Постановления Правительства РФ от 01.11.2012г. №1119 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

3.3.2. Приказа ФСТЭК России от 18.12.2013 №21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

3.3.3. нормативно-методических документов ФСБ России;

3.3.4. нормативные документы Компании в области обеспечения информационной безопасности.

3.4. Сведения о лицах, осуществляющих обновление программных средств ИСПДн Компании, подлежат регистрации.

3.5. Требования по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн Компании, определяются в соответствии с актуальными для Компании угрозами безопасности персональных данных, определенными в Частной модели угроз безопасности персональных данных при их обработке в ИСПДн. Требования по обеспечению безопасности персональных данных определены в Частном техническом задании.

3.6. На основании Частного технического задания и Частной модели угроз безопасности персональных данных разрабатывается Технический проект.

Технический проект предназначен для реализации технических мер по защите персональных данных и включает следующие подсистемы:

3.6.1. антивирусной защиты;

3.6.2. межсетевого экранирования;

3.6.3. управления доступом;

3.6.4. регистрации и учета;

3.6.5. обеспечения целостности;

3.6.6. обнаружения вторжений;

3.6.7. анализа защищенности.

3.7. Обеспечение безопасности персональных данных также достигается путем проведения внутренних проверок состояния защиты персональных данных согласно плану, приведенному в Приложении № 3 к настоящему Положению.

3.8. Контроль за исполнением требований организационно-технической и эксплуатационной документации в ИСПДн, а также за соблюдением принимаемых мер по обеспечению безопасности персональных данных и уровня защищенности ИСПДн возлагается на Дирекцию по расчетам и ИТ.

IV. ПРАВИЛА ПРЕДОСТАВЛЕНИЯ ДОСТУПА РАБОТНИКОВ К ПЕРСОНАЛЬНЫМ ДАННЫМ

4.1. Список лиц, допущенных к обработке персональных данных и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение правил обработки персональных данных, определяется и утверждается Генеральным директором.

4.2. Дирекция по персоналу при принятии на работу, увольнении или изменении должностных обязанностей Работников не позднее чем в трехдневный срок подает изменения в список лиц, допущенных к обработке персональных данных.

4.3. Руководители структурных подразделений при приеме на работу не позднее 1 рабочего дня с момента приема Работника при необходимости обязаны инициировать внесение вновь принятого Работника в список лиц, допущенных к обработке персональных данных.

4.4. Дирекция по персоналу и Дирекция по расчетам и ИТ не реже одного раза в квартал проводят сверку действующей редакции списка лиц, допущенных к обработке персональных данных, с действующими должностными обязанностями

Работников, а также перечнем лиц, которым реализован допуск к работе с персональными данными на технических средствах ИСПДн Компании.

4.5. Работники Компании выполняют действия по обработке персональных данных в соответствии со служебной необходимостью и возложенными на работников функциями.

4.6. Работники вправе осуществлять обработку персональных данных в пределах, определенных служебными функциями, и только после подписания обязательства о неразглашении информации, содержащей персональные данные, (Приложение №1 к настоящему Положению), а также ознакомления под роспись с положениями локальных актов Компании по обработке и защите персональных данных.

4.7. Лица, получившие доступ к персональным данным, должны использовать эти данные лишь в целях, для которых они были получены, обязаны соблюдать режим конфиденциальности персональных данных, информировать Дирекцию по расчетам и ИТ об утечке персональных данных, о фактах нарушения порядка обращения с ними, о попытках несанкционированного доступа к персональным данным.

4.8. Приказом Генерального директора Компании назначается сотрудник, ответственный за организацию обработки и защиты персональных данных в Компании, являющийся ответственным за соблюдение настоящего Положения.

4.9. Лицам, допущенным к обработке персональных данных, запрещается:

- распространять и предоставлять персональные данные любым способом третьим лицам без получения соответствующего разрешения Генерального директора Компании в письменном виде или по электронной почте, а также за исключением случаев, установленных законодательством РФ;

- оставлять материальные носители с персональными данными в доступном для третьих лиц месте;

- формировать и хранить базы данных (картотеки, файловые архивы и др.), содержащие персональные данные, без согласования с руководителем структурного подразделения, полученного в письменном виде или по электронной почте;

- использовать персональные данные в целях, не связанных с исполнением своих должностных обязанностей;

- получать и обрабатывать персональные данные, отнесенные

законодательством РФ к специальной категории персональных данных (касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и др.), за исключением случаев, предусмотренных законодательством РФ.

4.10. Доступ в ИСПДн предоставляется путем наделения правом на доступ к соответствующим ресурсам и к прикладному программному обеспечению, обрабатывающему персональные данные.

4.11. Компания обеспечивает режим безопасности помещений, в которых размещены объекты ИСПДн Компании, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в них.

V. ВЫЯВЛЕНИЕ И ПРЕДОТВРАЩЕНИЕ НЕПРАВОМЕРНЫХ ДЕЙСТВИЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

5.1. Перечень мер и комплекс мероприятий, направленных на предотвращение неправомерного использования персональных данных в Компании включает в себя:

5.1.1. инструктаж по вопросам обеспечения безопасности обработки и защиты персональных данных, а также информационной безопасности для вновь принятых сотрудников. Данный инструктаж осуществляется сотрудниками Дирекции по персоналу;

5.1.2. регулярное доведение до сведения Работников информации о возможных ошибках при осуществлении обработки персональных данных, ответственности при их наступлении;

5.1.3. выявление совершенных в процессе выполнения служебных обязанностей действий, нарушающих требования работы с персональными данными;

5.1.4. признание этих действий (бездействий) в установленном порядке недействительными, предотвращение и возмещение вреда;

5.1.5. служебное расследование фактов неправомерного обращения с персональными данными и привлечение виновных к ответственности.

5.2. ИСПДн Компании осуществляет регистрацию информации об авторе изменений, вносимых в персональные данные при их обработке в системе, что позволяет установить и привлечь к ответственности виновное лицо в случае неправомерных действий с персональными данными.

VI. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Лица, виновные в нарушении норм, регулирующих защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном законодательством Российской Федерации.

6.2. Контроль над выполнением требований настоящего Положения осуществляется Дирекцией по расчетам и ИТ.

ООО «Орион Экспресс»

Приложение №1
к Положению о защите
персональных данных
в ООО «Орион Экспресс»

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных

Я, _____,
(Фамилия Имя Отчество)

с Положениями ООО «Орион Экспресс» «Об обработке персональных данных» и «О защите персональных данных» ознакомлен и обязуюсь:

1. осуществлять обработку персональных данных исключительно в целях исполнения своих должностных обязанностей, в пределах и объемах, необходимых для их исполнения;
2. не разглашать персональные данные субъектов, ставшие мне известными в связи с исполнением моих должностных обязанностей;
3. обеспечивать сохранность материальных носителей, содержащих персональные данные субъектов, хранение которых входит в мои должностные обязанности, ключей от сейфов (металлических шкафов), помещений;
4. информировать руководителя об утрате документов, материальных носителей, содержащих персональные данные субъектов, ключей от сейфов (металлических шкафов), помещений, о других фактах нарушения порядка обращения с ними, а также о попытках несанкционированного доступа к персональным данным;
5. использовать персональные данные субъектов лишь в целях, для которых они сообщены.

Об ответственности за разглашение персональных данных субъектов предупрежден(а). Мне известно, что нарушение этих требований может повлечь уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

_____ /_____
(подпись) (Фамилия И.О.)

«___» _____ 20__ г.

Экземпляр обязательства получил(а):

Сотрудник Дирекции по персоналу _____/ _____
(подпись) (Фамилия И.О.)

ООО «Орион Экспресс»

Приложение №2
к Положению о защите
персональных данных
в ООО «Орион Экспресс»

Формы уведомлений субъектов персональных данных

ООО «Орион Экспресс»

Кому: _____
(фамилия, имя, отчество)

Юридический адрес:
Российская Федерация, 107078, г. Москва
вн. тер.г. муниципальный округ Басманный,
Большой Харитоньевский пер., д. 24, стр. 11,
помещ. 4

Адрес: _____

УВЕДОМЛЕНИЕ
о блокировании персональных данных _____№_____

Уважаемый (ая) _____

Уведомляем Вас о том, что Оператор персональных данных ООО «Орион Экспресс», юридический адрес: Российская Федерация, 107078, г. Москва вн. тер.г. муниципальный округ Басманный, Большой Харитоньевский пер., д. 24, стр. 11, помещ. 4, произвел блокирование Ваших персональных данных, а именно:

_____,
(перечень персональных данных)

которые обрабатываются в целях: _____
(цель обработки персональных данных)

в связи с _____
(причина блокирования)

Дата блокирования _____

_____ _____/_____
(должность) (Ф.И.О.) (подпись)

ООО «Орион Экспресс»

Кому: _____
(фамилия, имя, отчество)

Юридический адрес:
Российская Федерация, 107078, г. Москва
вн. тер.г. муниципальный округ Басманный,
Большой Харитоньевский пер., д. 24, стр. 11,
помещ. 4

Адрес: _____

УВЕДОМЛЕНИЕ

о внесении изменений в персональные данные _____№_____

Уважаемый (ая) _____

Уведомляем Вас о том, что Оператор персональных данных ООО «Орион Экспресс», юридический адрес: Российская Федерация, 107078, г. Москва вн. тер.г. муниципальный округ Басманный, Большой Харитоньевский пер., д. 24, стр. 11, помещ. 4, внес следующие изменения в Ваши персональные данные:

Наименование	Исходные данные	Новые данные

на основании следующих документов: _____
(перечень документов)

Дата возобновления обработки: _____

Срок или условие прекращения обработки персональных данных:

_____

_____ _____ /_____
(должность) (Ф.И.О.) (подпись)

ООО «Орион Экспресс»

Кому: _____
(фамилия, имя, отчество)

Юридический адрес:
Российская Федерация, 107078, г. Москва
вн. тер.г. муниципальный округ Басманный,
Большой Харитоньевский пер., д. 24, стр. 11,
помещ. 4

Адрес: _____

УВЕДОМЛЕНИЕ

о прекращении обработки и уничтожении персональных данных _____№_____

Уважаемый (ая) _____

Уведомляем Вас о том, что Оператор персональных данных ООО «Орион Экспресс», юридический адрес: Российская Федерация, 107078, г. Москва вн. тер.г. муниципальный округ Басманный, Большой Харитоньевский пер., д. 24, стр. 11, помещ. 4,

руководствуясь: _____

_____
(правовое основание обработки персональных данных)

осуществлял обработку Ваших персональных данных, а именно:

_____,
(перечень персональных данных)

в целях _____
(цель обработки персональных данных)

с _____ по _____
(дата начала обработки) (дата конца обработки)

Обработка указанных персональных данных была прекращена в связи с

_____
(причина окончания обработки персональных данных)

По окончании обработки Ваши персональные данные были уничтожены.

_____ _____ /_____
(должность) (Ф.И.О.) (подпись)

ООО «Орион Экспресс»

Приложение №3
к Положению о защите
персональных данных
в ООО «Орион Экспресс»

План внутренних проверок состояния защиты персональных данных в ООО «Орион Экспресс»

№	Наименование проверки	Периодичность выполнения	Ответственные за выполнения
1	Плановый пересмотр Моделей угроз безопасности	Не реже одного раза в год	Дирекция по расчетам и ИТ
2	Контроль содержания имеющихся документов Компании, регламентирующих технические меры обеспечения безопасности ПДн	Не реже одного раза в год	Дирекция по расчетам и ИТ
3	Проверка качества знаний работников в вопросах обеспечения безопасности ПДн	Два раза в год	Дирекция по персоналу
4	Контроль за использованием средств защиты информации	Два раза в год	Дирекция по расчетам и ИТ
5	Контроль за обеспечением безопасности персональных данных, при их обработке без использования средств автоматизации	Ежеквартально	Руководители структурных подразделений Компании
6	Контроль за обеспечением безопасности персональных данных, при их обработке в информационных системах персональных данных	Ежеквартально	Дирекция по расчетам и ИТ
7	Проверка списка лиц, допущенных к обработке персональных данных	Ежеквартально	Дирекция по расчетам и ИТ совместно с Дирекцией по персоналу
8	Контроль содержания типовых форм документов, предполагающих и (или) допускающих содержание персональных данных	Постоянно	Правовой департамент

Приложение № 1
к Приказу № 127 от «20» июня 2023 г.

УТВЕРЖДАЮ
Временно исполняющий обязанности
Генерального директора
ООО «Телекарта»
_____ Я.А. Гладышева
«20» июня 2023 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ООО «Телекарта»

г. Москва 2023

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированное рабочее место (АРМ) – совокупность оборудования (персональный компьютер, ноутбук, принтер и т.п.) и установленного на нем программного обеспечения, принадлежащего Компании и предназначенного для автоматизации деятельности работников Компании.

Актив – все, что имеет ценность для Компании и находится в ее распоряжении. К активам могут относиться:

- работники (персонал), финансовые (денежные) средства, средства вычислительной техники, телекоммуникационные средства и пр.;
- различные виды информации – платежная, финансово-аналитическая, служебная, управляющая, персональные данные и пр.;
- финансовые процессы;
- финансовые продукты и услуги, предоставляемые клиентам.

Доступность информационных активов – свойство информационной безопасности Компании, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

Жизненный цикл (ЖЦ) – совокупность взаимосвязанных процессов создания и последовательного изменения состояния автоматизированной системы от формирования исходных требований к ней до окончания эксплуатации и утилизации комплекса средств автоматизации.

Информационная инфраструктура (ИТ-инфраструктура) – система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия.

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для Компании и находящаяся в ее распоряжении, представленная на любом материальном носителе в форме, пригодной для ее обработки, хранения и передачи.

Инцидент информационной безопасности – событие или комбинация событий, указывающая на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности (далее – ИБ), результатом которой являются:

- нарушение или возможное нарушение работы средств защиты информации (далее – СЗИ) в составе системы обеспечения информационной безопасности (далее – СОИБ) Компании;
- нарушение или возможное нарушение требований законодательства Российской Федерации, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов Компании в области обеспечения ИБ, нарушение или возможное нарушение в выполнении процессов СОИБ Компании;

– нарушение или возможное нарушение в выполнении платежных и технологических процессов Компании;

– нанесение или возможное нанесение ущерба Компании и (или) ее клиентам.

Конфиденциальность информационных активов – свойство ИБ Компании, состоящее в том, что обработка, хранение и передача Информационных активов осуществляются таким образом, что Информационные активы доступны только авторизованным пользователям, отдельным модулям Автоматизированных систем или процессам.

Локальная вычислительная сеть (ЛВС) – группа средств вычислительной техники и связанных с ними устройств, соединенных средствами и линиями связи.

Нарушитель информационной безопасности – субъект, реализующий угрозы ИБ Компании.

Несанкционированный доступ (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или Автоматизированными системами.

Обработка информации – любое действие (операция) или совокупность действий (операций) с информацией, совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации.

Пользователь – работник Компании, допущенный к работе с информационными ресурсами Компании в рамках выполнения своих должностных обязанностей.

Привилегированные пользователи – к привилегированным пользователям относятся администраторы баз данных, разработчики программного обеспечения, сотрудники, занимающиеся технической поддержкой в сфере информационных технологий и другие сотрудники, должностные обязанности которых предусматривают расширенный либо неограниченный доступ к Информационным активам Компании.

Риск – мера, учитывающая вероятность реализации угрозы ИБ и величину потерь (ущерба) от реализации этой угрозы.

Роль – заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом.

СИБ – система информационной безопасности; совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

СМИБ – система менеджмента информационной безопасности; часть менеджмента Компании, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования ИБ Компании.

СОИБ – система обеспечения информационной безопасности; совокупность СИБ и СМИБ.

Стратегические улучшения СОИБ – корректирующие или превентивные действия, связанные с пересмотром Политики ИБ и Частных политик ИБ Компании, с последующим выполнением соответствующих тактических улучшений СОИБ.

Тактические улучшения СОИБ – корректирующие или превентивные действия, связанные с пересмотром отдельных процедур выполнения деятельности в рамках СОИБ Компании и не требующие пересмотра политики ИБ и Частных политик ИБ Компании.

Целостность информационных активов – свойство ИБ Компании сохранять неизменность или исправлять обнаруженные изменения в своих Информационных активах.

Угроза – угроза нарушения свойств ИБ – доступности, целостности или конфиденциальности Информационных активов Компании.

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

АРМ	–	Автоматизированное рабочее место
АС	–	Автоматизированная система
ЖЦ	–	Жизненный цикл
ЗИ	–	Защита информации
ИБ	–	Информационная безопасность
ИС	–	Информационная система
ИТ	–	Информационные технологии
КИ	–	Конфиденциальная информация
ЛВС	–	Личная вычислительная сеть
НСД	–	Несанкционированный доступ
ПДн	–	Персональные данные
РФ	–	Российская Федерация
СВТ	–	Средство вычислительной техники
СЗИ	–	Средство защиты информации
СИБ	–	Система информационной безопасности
СМИБ	–	Система менеджмента информационной безопасности
СОИБ	–	Система обеспечения информационной безопасности
ТЗ	–	Техническое задание

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика определяет общие направления, цели и задачи обеспечения информационной безопасности ООО «Телекарта» (далее – Компания), а также основные принципы и общие требования к организации процессов обеспечения информационной безопасности в Компании.

1.2. Настоящая Политика разработана в соответствии с требованиями законодательства РФ, нормативно-методических документов государственных регуляторов в сфере ИБ и международных стандартов.

1.3. Основополагающими принципами организации системы информационной безопасности Компании является согласованность нормативных документов Компании по обеспечению информационной безопасности и непротиворечивость их положений требованиям настоящей Политики.

1.4. Требования настоящей Политики и внутренних нормативных документов Компании, разработанных на ее основе, обязательны для исполнения всеми работниками Компании.

1.5. Положения настоящей Политики доводятся до сведения работников всех подразделений Компании.

1.6. Настоящая Политики утверждается Генеральным директором Компании и вводится в действие Приказом по Компании.

2. ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ ДОКУМЕНТОВ

2.1. Настоящая Политика разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения ИБ федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, в том числе:

- Доктриной информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 05.12.2016 г. № 646);
- Федеральным законом Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Информация является одним из наиболее важных и ценных активов, использующихся в деятельности Компании. Руководство Компании, в полной мере осознавая значимость Информационных активов, считает одной из приоритетных задач обеспечение ИБ Компании.

3.2. Целями обеспечения информационной безопасности определены:

- достижение адекватной защищенности интересов Компании в условиях угроз в информационной сфере и минимизации рисков ИБ;
- защита субъектов информационных отношений Компании от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи;
- минимизация уровня операционного и других рисков (риск нанесения ущерба деловой репутации Компании, правовой риск и т.д.);
- обеспечение непрерывности ведения бизнеса Компании.

3.3. Указанные цели достигаются посредством обеспечения и постоянного поддержания свойств ИБ (конфиденциальности, целостности, доступности) защищаемых Информационных активов, обрабатываемых Компанией во всех видах и формах, независимо от типа их носителя.

3.4. Для достижения целей обеспечения ИБ Компания обеспечивает эффективное решение следующих задач:

- формирование и совершенствование гибкой СИБ, включающей в себя комплекс организационных и технических мер по обеспечению безопасности, как самих Информационных активов, так и средств, и методов их обработки, в том числе хранения, модификации, передачи и т.д.;
- формирование и совершенствование СМИБ, в том числе процессов проверки и оценки СОИБ в целях повышения эффективности СОИБ;
- своевременное выявление и устранение уязвимостей Информационных активов Компании и среды их обработки, позволяющее предупредить возможности нанесения ущерба и нарушения нормального функционирования бизнес-процессов Компании в результате реализации угроз ИБ;
- уменьшение до приемлемого уровня возможного ущерба Компании при реализации угроз ИБ, в том числе сокращение времени восстановления технологических процессов после возможных прерываний;
- защита от вмешательства в процесс функционирования ЛВС Компании посторонних лиц;
- своевременное выявление и устранение инцидентов ИБ, в том числе неправомерного использования Информационных активов Компании;
- обеспечение соответствия технологических процессов Компании требованиям нормативных документов РФ в области обеспечения ИБ;

– предотвращение возникновения конфликта интересов при использовании и обеспечении безопасности Информационных активов Компании, а также условий для его возникновения;

– защита законных прав Компании, его работников в случае неправомерного использования Информационных активов Компании;

– планирование и оптимизация затрат на обеспечение информационной безопасности Компании на основе оценки рисков ИБ.

3.5. Поставленные основные цели обеспечения ИБ и решение задач обеспечения ИБ достигаются:

– строгим учетом всех подлежащих защите ресурсов ИС Компании (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

– журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств корпоративной ИС;

– полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Компании по вопросам обеспечения безопасности информации;

– подготовкой должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;

– наделением каждого работника (Пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Компании;

– четким знанием и строгим соблюдением всеми Пользователями ИС Компании требований организационно-распорядительных документов по вопросам обеспечения ИБ;

– персональной ответственностью за свои действия каждого работника, имеющего доступ к информационным ресурсам Компании, в рамках своих функциональных обязанностей;

– непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Компании;

– применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

– эффективным контролем над соблюдением Пользователями информационных ресурсов Компании требований по обеспечению ИБ;

– юридической защитой интересов Компании при взаимодействии ее подразделений с внешними организациями (связанным с обменом информацией) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

4. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Основные принципы обеспечения информационной безопасности.

При построении и обеспечении информационной безопасности Компания руководствуется рядом основополагающих принципов:

- Своевременность обнаружения проблем – Компания должна своевременно обнаруживать проблемы, потенциально способные негативно повлиять на ее бизнес-процессы;
- Прогнозируемость развития проблем – Компания должна выявлять причинно-следственную связь возможных проблем и строить на этой основе точный прогноз их развития;
- Оценка влияния проблем на бизнес-процессы – Компания должна адекватно оценивать степень влияния выявленных проблем на ее бизнес-процессы;
- Адекватность защитных мер – Компания должна выбирать защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от реализации угроз;
- Эффективность защитных мер – Компания должна эффективно реализовывать принятые защитные меры;
- Использование опыта при принятии и реализации решений – Компания должна накапливать, обобщать и использовать свой опыт на всех уровнях принятия решений и их исполнения;
- Непрерывность безопасного функционирования – Компания должна обеспечивать непрерывность реализации принципов безопасного функционирования;
- Контролируемость защитных мер – Компания должна применять только те защитные меры, правильность и эффективность работы которых может быть проверена, при этом Компания должна регулярно оценивать адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на бизнес-процессы Компании.

5. ПРЕДМЕТ ЗАЩИТЫ

5.1. Предметом защиты является информация, представленная в электронном виде или на материальном носителе (далее – информация), а также связанные с ней технические средства, процессы, программы, влияющие на защищенность информации.

5.2. Информационные активы Компании – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для Компании, находящаяся в распоряжении Компании и предоставленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

К информационным активам Компании в том числе относятся сведения, относящиеся к коммерческой тайне, персональные данные.

5.3. Сведения, относящиеся к коммерческой тайне – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых Компанией введен режим коммерческой тайны.

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

5.5. Кроме этого, защите может подлежать любая другая информация, которая, по мнению ее собственника или владельца (если ему такие права делегированы собственником), должна быть защищена от тех или иных угроз.

6. ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Обеспечение ИБ активов Компании и минимизация рисков ИБ осуществляются путем реализации, эксплуатации и совершенствования СОИБ в соответствии с положениями настоящей Политики.

6.2. СОИБ Компании представляет собой логически взаимосвязанную совокупность:

- защитных мер и средств, реализующих обеспечение ИБ Компании, и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение;
- процессов менеджмента ИБ, включая ресурсное и административное (организационное) обеспечение этих процессов.

6.3. СОИБ должна рассматриваться как важная и неотъемлемая составная часть общей безопасности Компании.

6.4. Основой для построения СОИБ Компании являются:

- требования законодательства РФ;
- договорные обязательства Компании;
- условия ведения бизнеса, выраженные на основе классификации активов Компании и оценки рисков ИБ.

6.5. Реализация, эксплуатация, контроль и поддержание на должном уровне СОИБ в Компании осуществляется ИТ-директором который является лицом, ответственным за функционирование системы обеспечения ИБ Компании.

6.6. Ответственные работники Компании в рамках их полномочий организуют и контролируют выполнение всех мероприятий по обеспечению ИБ Компании, направленных на снижение рисков ИБ и управление ими, организуют создание и эксплуатацию СОИБ, а также эксплуатацию АС в соответствии с правилами и требованиями, задаваемыми СОИБ.

6.7. Задачами работников Компании, ответственных за ИБ, являются:

- менеджмент инцидентов ИБ:
  - сбор информации о событиях ИБ;
  - выявление и анализ инцидентов ИБ;
  - расследование инцидентов ИБ;
  - оперативное реагирование на инцидент ИБ;
  - поддержка базы инцидентов ИБ и документирование всех расследований инцидентов безопасности;
  - минимизация негативных последствий инцидентов ИБ;
  - прогнозирование и предупреждение инцидентов ИБ;
  - оперативное доведение до руководства Компании информации по наиболее значимым инцидентам ИБ и оперативное принятие решений по ним;
  - выполнение принятых решений по всем инцидентам ИБ в установленные сроки;

- пересмотр применяемых требований, мер и механизмов по обеспечению ИБ по результатам рассмотрения инцидентов ИБ;
- разработка оптимальных процедур реагирования на инциденты ИБ и регламентирование порядка реагирования на инциденты ИБ;

– определение потребностей Компании в применении мер обеспечения ИБ, определяемых внутренними корпоративными требованиями;

– обеспечение эксплуатации средств и механизмов обеспечения ИБ:
- планирование применения, выбор, участие в тестировании и поставке средств обеспечения ИБ в Компании;
- эксплуатация средств обеспечения ИБ в Компании;

– разработка и пересмотр внутренних нормативных документов по обеспечению ИБ Компании, включая планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды внутренних нормативных документов;

– обучение, контроль и непосредственная работа с персоналом Компании в области обеспечения ИБ;

– выявление и предотвращение реализации угроз ИБ, пресечение несанкционированных действий нарушителей ИБ;

– организация проведения регулярного внешнего аудита ИБ Компании с целью оценки ИБ, включая оценку полноты и достаточности защитных мер и видов деятельности по обеспечению ИБ Компании;

– информирование руководства Компании и руководителей ее структурных подразделений об угрозах ИБ, влияющих на деятельность Компании.

6.8. Для выработки и проведения единой, согласованной политики в области ИТ и минимизации возможного ущерба Компании в случае реализации угроз ИБ, руководство Компании должно рассматривать вопросы ИТ с учетом их возможного влияния на компьютерную безопасность Компании.

6.9. Представляемые руководству Компании материалы по вопросам ИТ должны включать:

– предложения по обеспечению компьютерной безопасности при решении рассматриваемого вопроса;

– материалы по оценке стоимости проекта ИТ с учетом затрат по обеспечению компьютерной безопасности.

6.10. Вопросы выбора, закупки и внедрения средств для осуществления ЗИ, а также договоры и ТЗ на проведение работ по обеспечению компьютерной безопасности должны быть обязательно согласованы с ИТ-директором.

6.11. Реализация технических мероприятий по обеспечению ИБ и разграничению доступа к Информационным активам Компании осуществляется ИТ-директором Компании в соответствии с установленными требованиями.

6.12. Руководители структурных подразделений Компании организуют и контролируют выполнение требований ИБ в рамках своих подразделений, взаимодействуя с ИТ-директором по вопросам обеспечения ИБ.

6.13. Все подразделения Компании, создающие, использующие или хранящие защищаемые Информационные активы, принимают участие в планировании и реализации мероприятий (процессов) по обеспечению ИБ этих активов.

6.14. Основными задачами работников Компании при выполнении возложенных на них обязанностей и в рамках их участия в оперативной деятельности по обеспечению ИБ Компании являются:

- соблюдение требований ИБ, устанавливаемых нормативными документами Компании;
- выявление и предотвращение реализации угроз ИБ в пределах своей компетенции;
- выявление и реагирование на инциденты ИБ;
- информирование в установленном порядке ответственных лиц Компании о выявленных угрозах и рисковых событиях ИБ;
- прогнозирование и предупреждение инцидентов ИБ в пределах своей компетенции;
- мониторинг и оценка ИБ в рамках своего участка работы (рабочего места, структурного подразделения) и в пределах своей компетенции;
- информирование своего руководства и ИТ-директора о выявленной угрозе в информационной среде Компании.

7. СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

7.1. Общие требования по обеспечению ИБ Компании.

Требования ИБ формируются для следующих процессов (направлений) защиты информации:

- Обеспечение защиты информации при управлении доступом;
- Обеспечение защиты вычислительных сетей;
- Контроль целостности и защищенности информационной инфраструктуры;
- Защита от вредоносного кода;
- Предотвращение утечек информации;
- Управление инцидентами защиты информации;
- Использование корпоративной электронной почты;
- Повышение осведомленности сотрудников Компании в области ИБ.

7.2. **Требования по обеспечению защиты информации при управлении доступом.**

- *Управление учетными записями и правами субъектов логического доступа.*

Применяемые Компанией меры по управлению учетными записями и правами субъектов логического доступа должны обеспечивать:

- организацию и контроль использования учетных записей субъектов логического доступа;
- организацию и контроль предоставления (отзыва) и блокирования логического доступа;
- регистрацию событий защиты информации, связанных с операциями с учетными записями и правами логического доступа, и контроль использования предоставленных прав логического доступа.

- *Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа.*

Применяемые Компанией меры по идентификации, аутентификация, авторизации (разграничению доступа) при осуществлении логического доступа должны обеспечивать:

- идентификацию и аутентификацию субъектов логического доступа;
- организацию управления и организацию защиты идентификационных и аутентификационных данных;
- авторизацию (разграничение доступа) при осуществлении логического доступа;
- регистрацию событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией при осуществлении логического доступа.

- *Защита информации при осуществлении физического доступа.*

Применяемые Компанией меры по защите информации при осуществлении физического доступа должны обеспечивать:

- организацию и контроль физического доступа в помещения, в которых расположены объекты доступа;
- регистрацию событий, связанных с физическим доступом.

– *Идентификация и учет ресурсов и объектов доступа.*

Применяемые Компанией меры по идентификации и учету ресурсов и объектов доступа должны обеспечивать:

- организацию учета и контроль состава ресурсов и объектов доступа;
- регистрацию событий защиты информации, связанных с операциями по изменению состава ресурсов и объектов доступа.

7.3. **Требования по обеспечению защиты вычислительных сетей.**

– *Сегментация и межсетевое экранирование вычислительных сетей.*

Применяемые Компанией меры по сегментации и межсетевому экранированию вычислительных сетей должны обеспечивать:

- сегментацию и межсетевое экранирование внутренних вычислительных сетей;
- регистрацию событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей.

– *Выявление вторжений и сетевых атак.*

Применяемые Компанией меры по выявлению вторжений и сетевых атак должны обеспечивать:

- мониторинг и контроль содержимого сетевого трафика;
- регистрацию событий защиты информации, связанных с результатами мониторинга и контроля содержимого сетевого трафика.

– *Защита информации, передаваемой по вычислительным сетям.*

7.4. **Требования по контролю целостности и защищенности информационной инфраструктуры.**

Применяемые Компанией меры по контролю целостности и защищенности информационной инфраструктуры должны обеспечивать:

- контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации;
- организацию и контроль размещения, хранения и обновления ПО информационной инфраструктуры;
- контроль состава и целостности ПО информационной инфраструктуры;
- регистрацию событий защиты информации, связанных с результатами контроля целостности и защищенности информационной инфраструктуры.

7.5. **Требования по защите от вредоносного кода.**

Применяемые Компанией меры по защите от вредоносного кода должны обеспечивать:

- организацию и контроль применения средств защиты от вредоносного кода;
- регистрацию событий защиты информации, связанных с реализацией защиты от вредоносного кода.

7.6. **Требования по предотвращению утечек информации.**

Применяемые Компанией меры по предотвращению утечек информации должны обеспечивать:

- блокирование неразрешенных к использованию и контроль разрешенных к использованию потенциальных каналов утечки информации;
- контроль (анализ) информации, передаваемой по разрешенным к использованию потенциальным каналам утечки информации;
- организацию защиты машинных носителей информации (МНИ);
- регистрацию событий защиты информации, связанных с реализацией защиты по предотвращению утечки информации.

7.7. **Требования по управлению инцидентами защиты информации.**

– *Мониторинг и анализ событий защиты информации.*

Применяемые Компанией меры по мониторингу и анализу событий защиты информации должны обеспечивать:

- организацию мониторинга данных регистрации о событиях защиты информации, формируемых средствами и системами защиты информации, объектами информатизации;
- сбор, защиту и хранение данных регистрации о событиях защиты информации;
- анализ данных регистрации о событиях защиты информации;
- регистрацию событий защиты информации, связанных с операциями по обработке данных регистрации о событиях защиты информации.

– *Обнаружение инцидентов защиты информации и реагирование на них*

Применяемые Компанией меры по обнаружению инцидентов защиты информации и реагирование на них должны обеспечивать:

- обнаружение и регистрацию инцидентов защиты информации;
- организацию реагирования на инциденты защиты информации;
- организацию хранения и защиту информации об инцидентах защиты информации;
- регистрацию событий защиты информации, связанных с результатами обнаружения инцидентов защиты информации и реагирования на них.

7.8. **Требования к защите электронных сообщений.**

Применяемые Компанией меры должны обеспечивать:

- подписание электронных сообщений способом, позволяющим обеспечить их целостность и подтвердить их составление уполномоченным на это лицом.

7.9. **Требования по защите информации при использовании корпоративной электронной почты.**

Корпоративная почта предназначена исключительно для выполнения сотрудниками своих должностных обязанностей.

Все содержимое электронной почты является собственностью Компании.

Применяемые Компанией меры должны обеспечивать:

- возможность блокировки spam-сообщений;

- защиту от вредоносного кода на уровне почтового трафика;
- контроль (анализ) разрешенной к передаче информации на внешние адреса электронной почты и блокировка неразрешенной к передаче информации;
- контентный анализ почтового трафика;
- ограничение на перечень протоколов сетевого взаимодействия, используемых для осуществления передачи сообщений электронной почты;
- ограничение на перечень форматов файлов данных, разрешенных к передаче в качестве вложений в сообщения электронной почты;
- ограничение на размеры файлов данных, передаваемых в качестве вложений в сообщения электронной почты.

7.10. **Требования к повышению осведомленности работников Компании в области ИБ.**

Работники Компании должны периодически, но не реже одного раза в год, проходить повышение осведомленности, включая инструктажи и обучение, по порядку применения организационных мер защиты информации и использования технических средств защиты информации.

Компания должна обеспечивать:

- обучение, практическую подготовку (переподготовку) работников Компании, ответственных за применение мер защиты информации;
- повышение осведомленности (инструктаж) работников Компании в области защиты информации.

8. РЕАЛИЗАЦИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. В рамках СИБ Компании обеспечивается:

– разграничение доступа пользователей, обслуживающего персонала и третьих лиц к защищаемым Информационным активам Компании; средствам информатизации и коммуникациям, на которых обрабатывается (хранится, передается) защищаемая информация; СЗИ; помещениям, где размещены средства информатизации и коммуникации и (или) проводятся работы конфиденциального характера;

– физическая защита объектов информационной инфраструктуры Компании, обрабатывающих защищаемые информационные активы Компании;

– регистрация действий пользователей и обслуживающего персонала в АС, регистрация доступа обслуживающего персонала к телекоммуникационному и серверному оборудованию, СЗИ и т.д.;

– защита Информационных активов Компании от несанкционированных и нерегламентированных действий внешних и внутренних нарушителей, обрабатываемой и передаваемой СВТ и связи, и контроля утечки конфиденциальной информации за пределы ЛВС Компании;

– защита от несанкционированной модификации используемых в ЛВС Компании программных средств, а также защита объектов ЛВС Компании от внедрения несанкционированных программ, включая компьютерные вирусы;

– непрерывное и безопасное функционирование платежных и информационных технологических процессов, в рамках которых обрабатываются ПДн.

8.2. Реализация СИБ Компании достигается:

– регламентацией процессов обработки и ЗИ, действий работников, обслуживающего персонала Компании на основе организационно-распорядительных документов по вопросам обеспечения ИБ;

– обеспечением безопасности при управлении персоналом Компании, включая регламентацию процедур проверки кандидатов на работу, приема и увольнения работников Компании, проверки профессиональных навыков и оценки профессиональной пригодности работников Компании, применения мер дисциплинарного воздействия в отношении работников Компании за невыполнение требований ИБ;

– четким знанием и строгим соблюдением со стороны персонала, использующего и обслуживающего ресурсы Компании, требований нормативных документов Компании по вопросам обеспечения ИБ, в том числе за счет консультирования, повышения осведомленности и обучения персонала Компании по вопросам соблюдения требований ИБ;

– назначением и подготовкой (обучением) лиц, ответственных за организацию и осуществление мероприятий по обеспечению ИБ Компании и повышение уровня их профессиональных навыков;

– установлением ответственности за управление и использование Информационных активов Компании, а также за выполнение требований ИБ;

– разграничением потоков информации и запретом передачи конфиденциальной информации по незащищенным каналам связи;

– проведением организационных мероприятий и применением в составе используемых АС встроенных защитных мер, а также сертифицированных или разрешенных руководством Компании к применению СЗИ от НСД;

– применением технических СЗИ и регламентированием процессов их эксплуатации;

– строгим учетом всех подлежащих защите ресурсов Компании (информации, каналов связи, серверов, АРМ, сетевого оборудования, материальных носителей и т.д.);

– надежным хранением и уничтожением материальных носителей информации, исключающим их хищение, подмену и уничтожение;

– построением системы обработки инцидентов ИБ, включая оперативное реагирование на выявленные инциденты ИБ и минимизацию их последствий;

– резервным копированием защищаемых Информационных активов Компании и резервированием технических средств их обработки и защиты;

– осуществлением контроля функционирования средств и систем защиты информационных ресурсов Компании;

– управлением средствами и системами защиты информационных ресурсов Компании (управлением службами и процессами обеспечения ИБ);

– постоянным мониторингом информационной инфраструктуры Компании и текущего состояния ИБ, контролем использования и состояния информационной безопасности Информационных активов Компании на всех этапах ЖЦ, своевременным обнаружением и нейтрализацией внешних и внутренних угроз ИБ;

– проведением анализа эффективности и достаточности применяемых мер и средств ЗИ, возможных причин и последствий нарушения принципов непрерывности и безопасности операций, разработкой и реализацией предложений по совершенствованию СОИБ.

8.3. Сотрудниками, осуществляющими администрирование СЗИ, выполняется контроль выполнения требований эксплуатационной документации на используемые технические СЗИ в течение всего срока их эксплуатации.

9. СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

9.1. Реализация и функционирование СОИБ Компании основываются на «процесс-ориентированном подходе». Для реализации и поддержания ИБ в Компании реализуются четыре группы процессов, составляющих СМИБ Компании:

- планирование СОИБ («планирование»);
- реализация СОИБ («реализация»);
- мониторинг и анализ СОИБ («проверка»);
- совершенствование СОИБ («совершенствование»).

9.2. Группы процессов СМИБ Компании организуются в виде циклической модели «... – *планирование – реализация – проверка – совершенствование – планирование* – ...», которая является основой модели менеджмента ИБ Компании.

9.3. На этапе «Планирование» осуществляется формирование Политики ИБ, выполняется деятельность по определению области действия СОИБ и оценке рисков ИБ, проводится выбор и формируются планы реализации защитных мер (в том числе планы обработки рисков ИБ).

9.4. На этапе «Реализация» осуществляется выполнение всех планов, связанных с построением, вводом в действие, совершенствованием СОИБ и внедрением защитных мер. В том числе реализуется деятельность по обучению и повышению осведомленности в области ИБ работников Компании, обнаружению и реагированию на инциденты ИБ, обеспечению непрерывности бизнеса Компании.

9.5. На этапе «Проверка» проходит проверка соответствия выбранных защитных мер установленным требованиям ИБ, а также оценка соответствия ИБ Компании требованиям законодательства РФ, внутренним нормативным документам Компании.

9.6. Результат выполнения деятельности на этапе проверки является основой для выполнения деятельности по совершенствованию СОИБ, в рамках которой принимаются решения о реализации тактических и (или) стратегических улучшений СОИБ и определяются направления корректирующих и превентивных мер. При этом сама деятельность по совершенствованию СОИБ реализуется в рамках этапа реализации и при необходимости – планирования.

9.7. Менеджмент ИБ является частью общего корпоративного менеджмента Компании и ориентирован на содействие достижению бизнес-целей деятельности Компании путем обеспечения защищенности ее информационной инфраструктуры.

9.8. В рамках СМИБ Компании осуществляется анализ и оценка рисков ИБ, определяются оптимальные варианты обработки рисков для наиболее критичных информационных ресурсов и бизнес-процессов Компании, уточняются цели ИБ и область действия СОИБ, проводятся анализ и оценка эффективности функционирования СОИБ, определяются и реализуются меры по улучшению ИБ.

9.9. Деятельность СМИБ Компании обеспечивает достижение целей по обеспечению ИБ в условиях:

- штатного функционирования Компании;

– возникновения локальных инцидентов и проблем ИБ;

– возникновения широкомасштабных катастроф и аварий различной природы, последствия которых могут иметь отношение к ИБ Компании.

10. ОБЛАСТЬ ДЕЙСТВИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.1. В область действия СОИБ Компании должны входить все Информационные активы, включая конфиденциальную и открытую (общедоступную) информацию, принадлежащие Компании и (или) обрабатываемые Компанией, реализация угроз в отношении которых может нанести ущерб Компании, а также соответствующие им объекты ИТ-инфраструктуры Компании.

10.2. Определение области действия СОИБ (формирование перечней Информационных активов и объектов среды) осуществляется по итогам инвентаризации и классификации Информационных активов Компании. При этом состав информационных активов, входящих в область действия СОИБ, не должен противоречить нормам законодательства РФ.

10.3. По итогам классификации Информационных активов Компании для каждого класса информации должны быть определены требования и процедуры по их использованию и защите, поскольку для различных классов информации требуются различные уровни обеспечения безопасности.

10.4. Приоритеты в обеспечении ИБ классов Информационных активов определяются исходя из их ценности (значимости) для Компании.

10.5. Деятельность Компании поддерживается ИТ-инфраструктурой, которая обеспечивает автоматизацию технологических процессов и может быть представлена в виде иерархии следующих основных уровней:

- физический (линии связи, аппаратные средства и прочее);
- сетевое оборудование (маршрутизаторы, коммутаторы, концентраторы и пр.);
- сетевые приложения и сервисы;
- операционные системы;
- системы управления базами данных;
- технологические процессы и приложения;
- бизнес-процессы Компании.

10.6. Компания обеспечивает надлежащую защиту свойств ИБ (конфиденциальности, целостности, доступности) Информационных активов на каждом из уровней иерархии ИТ-инфраструктуры. При этом обеспечение свойств ИБ для Информационного актива заключается в создании необходимой защиты соответствующих ему объектов среды путем уменьшения или полного закрытия уязвимостей данного объекта за счет использования защитных мер.

10.7. Основными объектами ИТ-инфраструктуры Компании, подлежащими защите, являются:

- информационные активы, необходимые для работы Компании, независимо от формы и вида их представления;
- информационные технологии, технические и программные средства обработки информации в составе ИТ-инфраструктуры Компании;

– объекты размещения технических средств ИТ-инфраструктуры Компании;

– технологические процессы обработки информации в Компании;

– пользователи АС Компании.

10.8. К основным особенностям функционирования ИТ-инфраструктуры Компании относятся:

– большое разнообразие решаемых задач и типов обрабатываемых данных;

– объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;

– наличие каналов подключения к внешним сетям;

– наличие подсистем с различными требованиями к уровням защищенности, физически объединенных в единую ЛВС;

– разнообразие категорий пользователей и обслуживающего персонала;

– непрерывность функционирования;

– наличие требования обеспечения ИБ к ИТ-инфраструктуре Компании, включая требования Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности России.

11. УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

11.1. В целях создания эффективной СОИБ, достижения адекватной защищенности Информационных активов Компании и соответствующих им объектов среды в Компании реализуется деятельность по управлению рисками ИБ, которая является неотъемлемой частью всей деятельности по обеспечению ИБ Компании и применяется как при внедрении, так и при текущем функционировании СОИБ.

11.2. Управление рисками ИБ представляет собой непрерывный процесс, в рамках которого проводится анализ возможных сценариев развития событий, а также возможных последствий, после чего принимаются решения о предпочтительных сроках и мерах, которые следует предпринять для уменьшения риска до приемлемого уровня путем предотвращения возникновения угроз ИБ и (или) минимизации последствий в случае их реализации.

11.3. Подход к управлению рисками ИБ должен быть согласован с общим подходом к управлению рисками ИБ и соответствовать среде функционирования Компании.

11.4. Меры, принимаемые в области обеспечения ИБ, должны быть направлены на выявляемые риски ИБ эффективным и своевременным образом в тех местах и в такое время, когда они необходимы.

12. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИХ ИСТОЧНИКИ

12.1. На каждом из уровней ИТ-инфраструктуры Компании угрозы и их источники (в том числе злоумышленные), методы и средства защиты являются различными.

12.2. Основными угрозами безопасности информации, обрабатываемой в Компании, являются:

– нарушение конфиденциальности (разглашение, утечка) сведений, составляющих коммерческую тайну, в том числе персональных данных, а также инсайдерскую информацию;

– нарушение работоспособности (доступности) ЛВС, критичных АРМ и серверов Компании, выражающейся в блокировании информации, срыве своевременного решения задач, нарушении технологических процессов;

– нарушение целостности (искажение, подмена, уничтожение) информационных активов Компании и ключевых элементов среды их обработки.

12.3. В Компании рассматриваются источники угроз природного, техногенного и антропогенного характера. При этом источники угроз антропогенного характера (нарушители ИБ) могут быть как злоумышленные, так и незлоумышленные.

12.4. Целью злоумышленников является получение контроля над Информационными активами Компании, приводящего к нарушению их свойств конфиденциальности, целостности или доступности. Для достижения этой цели злоумышленник может использовать все способы проведения атак на всех уровнях ИТ-инфраструктуры Компании.

12.5. Любое лицо, имеющее физический и логический доступ к Информационным активам и компонентам ИТ-инфраструктуры Компании (ПО и данным, СВТ, коммуникационному оборудованию и каналам связи), является потенциальным злоумышленником, способным нанести ущерб Компании.

12.6. Основными источниками угроз ИБ в Компании являются:

– внутренние нарушители: работники Компании, имеющие доступ к информационным активам Компании, обслуживающий и технический персонал Компании, реализующие угрозы ИБ в рамках легально предоставленных им прав и полномочий и за их пределами;

– внешние нарушители ИБ: лица, не являющиеся работниками Компании (конкуренты, хакеры, террористы, криминальные элементы и т.п.), но осуществляющие попытки НСД к информационным активам Компании;

– комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие совместно и (или) согласованно;

– неблагоприятные события природного, техногенного и социального характера;

– сбои, отказы, разрушения/повреждения программных и технических средств;

– зависимость от поставщиков/провайдеров/партнеров;

– несоответствие требованиям надзорных и регулирующих органов, действующего законодательства РФ.

12.7. Для эффективного обеспечения ИБ Информационных активов Компании на всех уровнях иерархии ИТ-инфраструктуры Компании на регулярной основе проводится работа по выявлению и анализу актуальных для Компании угроз ИБ и их источников, результаты которой документируются в виде моделей угроз и нарушителей ИБ.

12.8. Модель угроз ИБ включает описание источников угроз, уязвимостей, которые используются угрозами, методов и объектов нападений, типов возможных потерь (например, конфиденциальности, целостности, доступности активов), масштаба потенциального ущерба. Степень детализации параметров моделей угроз и нарушителей ИБ может быть различна и определяется реальными потребностями Компании.

12.9. Модель угроз ИБ включает перечень угроз, характерных для того или иного уровня иерархии ИТ-инфраструктуры.

12.10. Модель нарушителя ИБ включает описание опыта нарушителя, доступных ресурсов, необходимых для реализации угрозы, времени и места действия и возможной мотивации его действий.

12.11. Модели угроз и нарушителей являются основными инструментами Компании при развертывании, поддержании и совершенствовании СОИБ.

12.12. На основе модели угроз и нарушителей ИБ производятся анализ и оценка рисков ИБ, разрабатываются варианты обработки рисков для наиболее критичных информационных ресурсов и бизнес-процессов Компании.

12.13. Модели угроз и нарушителей могут разрабатываться как для ЛВС Компании в целом, так и для ее отдельных компонентов.

13. ПРОВЕРКА И ОЦЕНКА СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

13.1. В целях контроля и поддержания в актуальном состоянии СОИБ с учетом изменений требований и приоритетов бизнеса, появления новых угроз и уязвимостей, снижения эффективности существующих мер защиты в Компании на регулярной основе реализуются мероприятия по проверке и оценке СОИБ Компании.

13.2. Проверка и оценка СОИБ Компании проводится путем выполнения следующих процессов:

- мониторинг и контроль защитных мер (в том числе контроль соблюдения работниками Компании требований ИБ);
- оценка соответствия ИБ;
- анализ функционирования СОИБ (в том числе со стороны руководства Компании).

13.3. Мониторинг и контроль защитных мер проводятся ответственными работниками в рамках их полномочий под руководством ИТ-директора, с целью оперативной проверки работоспособности и эффективности мер обеспечения ИБ.

13.4. Мониторинг и контроль защитных мер заключаются в оперативном и постоянном наблюдении, сборе, анализе и обработке данных о событиях, относящихся к ИБ, с целью:

- обнаружения, регистрации и устранения отклонений функционирования защитных мер от требований ИБ;
- контроля и оценки полноты реализации положений настоящей Политики и документов, разработанных на ее основе;
- выявление нештатных, в том числе злоумышленных, действий в информационной системе Компании и инцидентов ИБ.

13.5. В случае обнаружения инцидентов нарушения ИБ в Компании выполняются процедуры управления инцидентами.

13.6. Оценка соответствия ИБ является одним из основных средств проверки и оценки (контроля) реализуемых в Компании организационных и технических мер ЗИ.

13.7. Оценка соответствия ИБ Компании выполняется в форме:

- аудита ИБ – проводится внешними по отношению к Компании независимыми проверяющими организациями;
- самооценки ИБ – проводится силами работников Компании.

13.8. Аудит и самооценка ИБ проводятся в Компании в целях:

- оценки достаточности и эффективности реализованных в Компании мер по обеспечению ИБ и их соответствия требованиям законодательства РФ, российских стандартов в области ИБ, а также требованиям внутренних документов Компании по обеспечению ИБ;
- выявления уязвимостей в СИБ Компании и принятия мер по их устранению;
- предоставления гарантий защищенности информационных ресурсов Компании от угроз ИБ.

13.9. Помимо собственных (внутренних) целей Компании Аудит ИБ проводится также с целью повышения доверия к Компании со стороны партнеров и иных организаций.

13.10. Цель, порядок и периодичность проведения отдельных аудитов и самооценок ИБ Компании (отдельных структурных подразделений Компании) определяются руководством Компании на основе потребностей в такой деятельности и фиксируются в программе аудитов и самооценок ИБ.

13.11. Ответственность за разработку и реализацию программ аудитов и самооценок ИБ возлагается на ИТ-директора.

13.12. По результатам мониторинга, контроля и оценки соответствия ИБ должны проводиться анализ функционирования СОИБ и оценка выявленных нарушений и отклонений от требований нормативных документов Компании в области обеспечения ИБ. Результаты анализа должны доводиться до руководства Компании.

13.13. Анализ функционирования СОИБ проводится ИТ-директором, а также ответственными работниками Компании, в том числе на основании подготавливаемых ИТ-директором документов (данных).

13.14. Основными целями проведения анализа функционирования СОИБ являются:

- оценка эффективности СОИБ;
- оценка соответствия СОИБ требованиям законодательства РФ;
- оценка соответствия СОИБ существующим и возможным угрозам ИБ;
- оценка следования принципам ИБ и выполнения требований обеспечения ИБ, закрепленным в настоящей Политике и иных внутренних документах Компании.

13.15. По результатам анализа функционирования СОИБ в Компании принимаются решения (в случае необходимости) по тактическим и стратегическим улучшениям СОИБ и назначаются ответственные за их реализацию. Реализация мероприятий по тактическим и стратегическим улучшениям контролируется ИТ-директором и руководством Компании.

13.16. Результаты, полученные в ходе проверки и оценки СОИБ, являются основой для устранения выявленных недостатков в обеспечении ИБ, корректировки настоящей Политики ИБ и совершенствования СОИБ в целом.

14. ОТВЕТСТВЕННОСТЬ

14.1. Ответственность за обеспечение ИБ Компании возлагается на все структурные подразделения Компании в рамках их полномочий и в соответствии с положениями, установленными настоящей Политикой и разработанными на ее основе документами Компании.

14.2. Руководители структурных подразделений несут ответственность:

– за своевременное доведение требований внутренних нормативных документов Компании в области ИБ до работников их подразделений в части их касающейся;

– за выделение Информационных активов Компании, подлежащих защите, владельцем которых являются их подразделения, а также согласование заявок на доступ к данным активам;

– за выполнение работниками их подразделений требований внутренних нормативных документов Компании в области ИБ.

14.3. Все работники Компании несут персональную ответственность за свои действия при работе в ИС Компании и обращении с защищаемыми информационными активами Компании, а также за выполнение требований ИБ, установленных настоящей Политикой и нормативными документами, разработанными на ее основе.

14.4. Ответственность за контроль исполнения и актуальность настоящей Политики, а также за внесение в нее изменений возлагается на ИТ-директора.

14.5. Обязанности работников Компании по выполнению требований ИБ отражаются в трудовых договорах и (или) должностных инструкциях работников Компании.

14.6. За нарушение требований настоящей Политики и документов Компании, разработанных на ее основе, предусмотрена ответственность в соответствии с внутренними нормативными документами Компании и законодательством РФ.

15. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

15.1. Настоящая Политика вступает в силу с даты утверждения.

15.2. Настоящая Политика должна пересматриваться не реже одного раза в год.

15.3. Предпосылкой для пересмотра настоящей Политики являются следующие изменения:

- в законодательстве Российской Федерации;
- интересов, целей и задач бизнеса Компании;
- организационной структуры Компании, а также по итогам расследования критичных инцидентов ИБ.

15.4. В случае возникновения как минимум одного из перечисленных выше изменений ИТ-директор инициирует процесс пересмотра требований настоящей Политики. До момента утверждения новой редакции настоящая Политика применяется в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также действующим внутренним документам Компании.

ЛИСТ ОЗНАКОМЛЕНИЯ
с Политикой информационной безопасности ООО «Телекарта»

№ п/п	ФИО	Должность	Дата	Подпись

Приложение № 2
к Приказу № 10 от «17» июля 2023 г.

УТВЕРЖДАЮ
Генеральный директор
ООО «Орион Экспресс»

К.И. Махновский

2023 г.

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
в ООО «Орион Экспресс»

г. Москва 2023

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение «Об обработке персональных данных» в ООО «Орион Экспресс» (далее – Положение) определяет политику, порядок и условия обработки персональных данных, а также устанавливает общие требования к обеспечению безопасности персональных данных, обрабатываемых в ООО «Орион Экспресс» (далее – Компания).

1.2. Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Налоговым кодексом РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», 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», Распоряжением Правительства РФ от 21.03.1994 № 358-р «Об обеспечении сохранности документов по личному составу» и иными нормативными актами, действующими на территории Российской Федерации.

1.3. В настоящем Положении используются следующие термины и определения:

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

Обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу (в том числе распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор персональных данных - 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.

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

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

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

Конфиденциальность персональных данных - обязательное для соблюдения оператором персональных данных или иным получившим доступ к персональным данным лицом требование не допускать их распространения или предоставления третьим лицам без согласия субъекта персональных данных или требования Федерального закона.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Работодатель – Компания, вступившая в трудовые отношения с работником и правовые отношения с соискателем на вакантную должность.

Работник – физическое лицо, вступившее в трудовые отношения с Компанией.

Кандидат на вакантную должность – физическое лицо, вступившее в правовые отношения с Компанией с целью устройства на работу в Компанию.

Клиент - физическое лицо, вступившее в договорные отношения по оказанию ему услуг, предоставляемых ООО «Орион Экспресс».

1.4. Настоящее Положение вступает в силу со дня его утверждения Генеральным Директором.

1.5. Настоящее Положение распространяется на все Персональные данные, обрабатываемые Компанией, и обязательно для применения всеми Работниками Компании, осуществляющими обработку Персональных данных в силу своих должностных обязанностей.

1.6. Настоящее Положение доводится до сведения всех Работников персонально под роспись.

1.7. Настоящее Положение является общедоступным, что обеспечивается путем его размещения на сайте Компании по адресу: www.orion-express.ru.

1.8. Информация об Операторе персональных данных:

Общество с ограниченной ответственностью «Орион Экспресс»

ИНН 7710582109 / ОГРН 1057746735980

Контактная информация:

Почтовый адрес: 123308, г. Москва, а/я 57

ООО «Орион Экспресс»

Телефон + 7 (495) 781-41-01

Электронная почта: info@orion-express.ru

II. ПЕРЕЧЕНЬ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Компанией осуществляется обработка персональных данных следующих категорий субъектов персональных данных:

2.1.1. Работники Компании, бывшие Работники Компании;

2.1.2. Родственники Работников;

2.1.3. Кандидаты на вакантную должность;

2.1.4. Клиенты;

2.1.5. Представители контрагентов;

2.1.6. Аффилированные лица, участники Компании и их представители;

2.1.7. Лица, выполняющие работы по гражданско-правовым договорам.

2.2. В зависимости от категории субъекта персональных данных Компания вправе обрабатывать следующие категории персональных данных:

2.2.1. В отношении Работников Компании, бывших Работников Компании:

- фамилия, имя, отчество;
- дата и год рождения;
- место рождения;
- адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания;
- номера телефонов (мобильного и домашнего);
- электронная почта;
- сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки;
- сведения о повышении квалификации и переподготовке;
- сведения о трудовой деятельности;
- трудовом стаже;
- сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;
- содержание и реквизиты трудового договора с работником или гражданско-правового договора с гражданином;
- сведения о заработной плате (банковские реквизиты счетов для расчета с Работниками, данные по окладу, надбавкам, налогам и другие сведения);
- сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии/снятии на (с) учет(а));
- сведения о номере страхового свидетельства государственного пенсионного страхования;
- сведения об идентификационном номере налогоплательщика;
- сведения, указанные в оригиналах и копиях приказов по личному составу Компании и материалах к ним;
- сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) Работников Компании;
- материалы по аттестации и оценке Работников Компании;
- материалы по внутренним служебным расследованиям в отношении Работников Компании;
- внутрикорпоративные материалы по разбирательству и учету

несчастных случаев на производстве и профессиональным заболеваниям в соответствии с Трудовым кодексом Российской Федерации, другими федеральными законами;

- сведения о временной нетрудоспособности работников Компании;
- табельный номер Работника Компании;
- наименование должности, дата приема на работу;
- сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения), о семейном положении, составе семьи, а также сведения о членах семьи.
- паспортные данные (серия, номер, кем и когда выдан).

2.2.2. В отношении Родственников Работников:

- фамилия, имя, отчество;
- дата и год рождения;
- место работы/учебы.
- место рождения;
- сведения о номере страхового свидетельства государственного пенсионного страхования;
- сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения);
- адрес места жительства, номер телефона, электронная почта.

2.2.3. В отношении Кандидатов на вакантную должность:

- фамилия, имя, отчество;
- дата и год рождения;
- место рождения;
- адрес места жительства;
- номер телефона;
- электронная почта;
- воинский учет;
- информация о семейном положении;
- сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки;
- сведения о повышении квалификации и переподготовке;
- сведения о трудовой деятельности, трудовом стаже;

- фотография;
- иные сведения, содержащиеся в резюме, сообщаемые Кандидатом.

2.2.4. В отношении Клиентов:

- фамилия, имя, отчество;
- номер телефона;
- электронная почта;
- паспортные данные (серия, номер, кем и когда выдан);
- адрес установки приемного оборудования, марка оборудования;
- номер карты доступа;
- банковские реквизиты для перечисления денежных средств (требуется в случае возврата денежных средств).

2.2.5. В отношении Представителей контрагентов:

- фамилия, имя, отчество;
- номер телефона;
- электронная почта;
- должность;
- адрес регистрации;
- паспортные данные (серия, номер, кем и когда выдан).

2.2.6. В отношении Аффилированных лиц, участников Компании и их представителей:

- фамилия, имя, отчество;
- паспортные данные (серия, номер: кем и когда выдан);
- дата и место рождения;
- сведения об идентификационном номере налогоплательщика;
- адрес регистрации, почтовый адрес;
- сведения о гражданстве;
- номер телефона и адрес электронной почты;
- доля участия в уставном капитале Компании.

2.2.7. В отношении Лиц, выполняющих работы по гражданско-правовым договорам:

- фамилия, имя, отчество;
- номер телефона;
- электронная почта;
- сведения об идентификационном номере налогоплательщика;

- банковские реквизиты (в целях расчета по договорам);
- паспортные данные (серия, номер, кем и когда выдан);
- адрес регистрации, номер СНИЛС

2.3. Персональные данные носят конфиденциальный характер. Работники Компании, имеющие доступ к персональным данным в силу своих должностных обязанностей, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством РФ.

2.4. Все персональные данные субъекта следует получать у него самого, за исключением случаев, если в силу закона их получение возможно у третьей стороны.

2.4.1. Получение персональных данных Работодателем о Работнике у третьих лиц, возможно только при уведомлении Работника об этом заранее и с его письменного согласия.

В письменном уведомлении Работодатель должен поставить Работника в известность о целях получения персональных данных, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных и последствиях отказа Работника дать письменное согласие на их получение.

2.5. Компания не имеет права получать и обрабатывать сведения о субъектах персональных данных, отнесенные законодательством РФ к специальной категории персональных данных, за исключением случаев, предусмотренных законодательством РФ.

2.5.1. Работодатель не имеет права получать и обрабатывать персональные данные Работника о его членстве в общественных объединениях, за исключением случаев, предусмотренных законодательством РФ.

2.6. Биометрические персональные данные могут обрабатываться Компанией только при наличии согласия в письменной форме субъекта персональных данных, если иное не установлено законодательством РФ.

Цветное фотоизображение лица Работника, которое может использоваться Компанией для размещения на сайте Компании в целях информирования потенциальных и существующих контрагентов, Клиентов о Работниках, производится с согласия Работника и обрабатывается Компанией только при наличии согласия в письменной форме субъекта персональных данных, если иное не

установлено законодательством РФ, и не используется Компанией в целях установления личности субъекта персональных данных.

2.7. Трансграничная передача персональных данных на территорию иностранных государств не производится.

2.8. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда субъекту персональных данных, затруднения реализации его прав и свобод.

2.9. При принятии решений, затрагивающих интересы субъекта персональных данных, Компания не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки.

III. ЦЕЛИ И ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка персональных данных Работников Компании, бывших Работников Компании (перечень обрабатываемых персональных данных указан в п. 2.2.1. настоящего Положения) осуществляется в целях: обеспечения трудовых и производственных процессов с соблюдением законов и иных нормативно-правовых актов РФ; организации обучения; организации командировок; получения ключей электронной подписи и сертификатов ключей проверки электронной подписи; оформления добровольного медицинского страхования; зарплатного проекта; оформления визитных карточек; осуществления возложенных на Компанию законодательством РФ функций и обязанностей; оформления доверенностей для выполнения Работником своих трудовых обязанностей.

3.2. Обработка персональных данных Родственников Работников Компании (перечень обрабатываемых персональных данных указан в п. 2.2.2. настоящего Положения) осуществляется в целях: осуществления возложенных на Компанию законодательством РФ функций и обязанностей; предоставления социальных льгот Работникам.

3.3. Обработка персональных данных Кандидатов на вакантную должность (перечень обрабатываемых персональных данных указан в п. 2.2.3. настоящего Положения) осуществляется в целях: подбора кандидатов на вакантную должность; организации собеседований.

3.4. Обработка персональных данных Клиентов (перечень обрабатываемых персональных данных указан в п. 2.2.4. настоящего Положения) осуществляется в целях: заключения и исполнения договора, стороной которого либо

выгодоприобретателем или поручителем по которому является субъект персональных данных; обработки запросов, связанных с указанными договорами, информирования по заключенным договорам; продвижения товаров и услуг Компании на рынке; оценки качества услуг.

3.5. Обработка персональных данных представителей контрагентов (перечень обрабатываемых персональных данных указан в п. 2.2.5. настоящего Положения) осуществляется в целях: проверки полномочий предстателя контрагента; взаимодействие с контрагентами Компании при ведении договорной работы (включая преддоговорную работу), при исполнении обязательств по договорам и соглашениям.

3.6. Обработка персональных данных Аффилированных лиц, участников Компании и их представителей (перечень обрабатываемых персональных данных указан в п. 2.2.6. настоящего Положения) осуществляется в целях: осуществления возложенных на Компанию законодательством РФ функций и обязанностей; осуществления деятельности Компании.

3.7. Обработка персональных данных Лиц, выполняющих работы по гражданско-правовым договорам (перечень обрабатываемых персональных данных указан в п. 2.2.7. настоящего Положения) осуществляется в целях: исполнения обязательств по договорам, осуществления возложенных на Компанию законодательством РФ функций и обязанностей.

3.8. Указанные в разделе 2 настоящего Положения персональные данные обрабатываются исключительно в объеме, требуемом для достижения целей их обработки.

3.9. Сведения согласно п. 2 ч. 1 ст. 18.1. Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» приведены в Приложении №1 к Положению.

3.10. Правовыми основаниями обработки Компанией персональных данных являются:

3.10.1. Конституция Российской Федерации;

3.10.2. Гражданский кодекс Российской Федерации;

3.10.3. Налоговый кодекс Российской Федерации;

3.10.4. Трудовой кодекс Российской Федерации;

3.10.5. Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;

3.10.6. Федеральный закон от 07.07.2003 №126-ФЗ «О связи»;

3.10.7. Федеральный закон от 08.02.1998 № 14-ФЗ «Об обществах с ограниченной ответственностью»;

3.10.8. Постановление Правительства РФ от 22.12.2006 № 785 «Об утверждении Правил оказания услуг связи для целей телевизионного вещания и (или) радиовещания»;

3.10.9. Закон РФ от 07.02.1992 № 2300-1 «О защите прав потребителей»;

3.10.10. Федеральный закон от 01.04.1996 г. №27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

3.10.11. Федеральный закон от 29.12.2006 № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;

3.10.12. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»

3.10.13. Федеральный закон от 28.03.1998 No 53-ФЗ «О воинской обязанности и военной службе»;

3.10.14. Устав Компании;

3.10.15. согласие субъекта персональных данных на обработку его персональных данных;

3.10.16. осуществление и выполнение возложенных законодательством РФ на Компанию функций, полномочий и обязанностей;

3.10.17. заключение и исполнение договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

3.10.18. лицензия на оказание услуг связи для целей эфирного вещания.

IV. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Обработка персональных данных ограничивается достижением определенных конкретных целей.

Персональные данные обрабатываются в объеме, требуемом для достижения цели их обработки.

4.2. При обработке персональных данных должны быть обеспечены точность и достаточность персональных данных, а в необходимых случаях и актуальность по отношению к целям их обработки.

4.3. Обработка персональных данных Компанией включает в себя следующие процессы:

4.3.1. получение (сбор);

4.3.2. уточнение (обновление, изменение);

4.3.3. систематизация, запись, накопление;

4.3.4. использование;

4.3.5. хранение;

4.3.6. передачу (распространение, предоставление, доступ);

4.3.7. обезличивание;

4.3.8. блокирование, удаление, уничтожение;

4.3.9. ведение видеонаблюдения, которое осуществляется с помощью технических средств, установленных в служебных помещениях Работодателя.

4.4. При обработке персональных данных должна быть обеспечена их Конфиденциальность, т.е. созданы условия, не допускающие их раскрытия и распространения без согласия субъекта персональных данных, за исключением случаев, предусмотренных законодательством РФ.

4.5. Компания вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено законодательством РФ. В случае, если Компания на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом Конфиденциальности персональных данных и безопасности персональных данных при их обработке. Кроме того в поручении на обработку персональных данных должны быть определены перечень персональных данных, перечень действий с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, требования, предусмотренные ч. 5 ст. 18 и ст. 18.1. Федеральным законом № 152-ФЗ «О персональных данных», а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федеральным законом № 152-ФЗ «О персональных данных», в том числе требование об уведомлении оператора в случаях, предусмотренных частью 3.1 статьи 21 Федерального закона № 152-ФЗ «О персональных данных». Компания может передавать персональные данные органам государственной власти и иным уполномоченным органам в соответствии с действующим законодательством РФ.

4.6. Обработка персональных данных в Компании может осуществляться как с использованием, так и без использования средств автоматизации.

4.7. Неавтоматизированная обработка персональных данных должна осуществляться таким образом, чтобы персональные данные обособлялись от иной информации, в частности, путем фиксации их на отдельных материальных носителях персональных данных и иными способами.

4.8. При сохранении персональных данных на материальных носителях не допускается сохранение на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы.

4.9. При обработке персональных данных Компания обеспечивает использование баз данных, находящихся на территории РФ.

Серверы базы данных Компании расположены на территории РФ, по адресу: 123308, г. Москва, ул. Демьяна Бедного, д.24, корпус 1.

V. СРОКИ ХРАНЕНИЯ И ТРЕБОВАНИЯ К УНИЧТОЖЕНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, если иной срок не установлен законом или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

5.2. Сроки обработки персональных данных определяются в соответствии со сроком, указанным в согласии субъекта персональных данных, сроком действия договора, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, а также иными сроками, установленными законодательством РФ.

5.3. Персональные данные, обрабатываемые в Компании, подлежат уничтожению (либо блокировке в случае невозможности уничтожения) в следующих случаях: при достижении целей обработки персональных данных или в случае утраты необходимости в их достижении, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Компанией и субъектом персональных данных либо если Компания не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных действующим законодательством РФ; в случае отзыва субъектом персональных данных согласия на обработку его персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Компанией и субъектом персональных данных либо если Компания не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных действующим законодательством РФ.

5.4. Уничтожение документов (носителей), содержащих персональные данные, производится путем сожжения, дробления (измельчения). Для уничтожения бумажных документов может быть использован шредер. Персональные данные на электронных носителях уничтожаются путем стирания или форматирования носителя.

5.5. В случае если обработка персональных данных осуществляется без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных.

В случае если обработка персональных данных осуществляется с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных.

5.6. В Компании создаются и хранятся документы, содержащие сведения о субъектах персональных данных. Требования к использованию в Компании данных типовых форм документов установлены Постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

VI. ПРАВА И ОБЯЗАННОСТИ

6.1. Права и обязанности Компании:

6.1.1. Обязанности Компании, как оператора персональных данных, определяются законодательством Российской Федерации в области персональных данных.

6.1.2. Компания, как оператор персональных данных, вправе:

- защищать свои права и интересы в судебных органах;
- в случаях, предусмотренных действующим законодательством Российской Федерации, предоставлять персональные данные субъектов персональных данных государственным и иным уполномоченным органам (налоговые, правоохранительные органы и др.);
- отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством Российской Федерации;
- обрабатывать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством Российской Федерации.

6.2. Права и обязанности субъекта персональных данных:

6.2.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

6.2.2. Субъект персональных данных имеет право на получение сведений, касающихся обработки его персональных данных, за исключением случаев, предусмотренных законодательством РФ. Компания при обращении или при получении запроса субъекта персональных данных или его законного представителя на предоставление информации о персональных данных о соответствующем субъекте обязана предоставить сведения, касающиеся обработки его персональных данных в доступной форме. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Компанией, либо сведения, иным образом подтверждающие факт обработки персональных данных Компанией, и собственноручную подпись субъекта персональных данных или его законного представителя. (Примеры форм запросов субъектов приведены в Приложении № 4 к настоящему Положению).

6.2.3. Субъект персональных данных имеет право на получение при обращении или при направлении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- 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;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

– иные сведения, предусмотренные законодательством РФ.

Оператор предоставляет указанные сведения субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

6.2.4. Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случаях, предусмотренных законодательством РФ.

6.2.5. Субъект персональных данных вправе требовать от Компании 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.

6.2.6. Запросы, обращения и требования субъектов по обработке их персональных данных регистрируются в «Журнале учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных ООО «Орион Экспресс» (Приложение № 5 к Положению).

6.2.7. Ответственным за реализацию обращений и требований субъектов персональных данных является ответственный за организацию обработки персональных данных, назначаемый приказом Генерального директора Компании.

6.2.8. После реализации запросов, обращений и требований субъектов персональных данных, Компания уведомляет субъекта о выполненных действиях.

6.2.9. Субъект персональных данных вправе в любой момент отозвать согласие на обработку его персональных данных. Такое уведомление может быть передано Компании в том числе, но не ограничиваясь, следующими способами:

– путем направления письменного уведомления по адресу: 123308, г. Москва, а/я 57, ООО «Орион Экспресс»;

– путем направления уведомления по адресу электронной почты info@orion-express.ru;

– путем направления уведомления через личный кабинет абонентов на сайте www.orion-express.ru;

– обратившись в ООО «Орион Экспресс» иными способами.

6.3. Субъекты персональных данных могут получить разъяснения по вопросам обработки своих персональных данных Компанией, направив соответствующий письменный запрос ответственному за обработку персональных данных лицу Компании по почтовому адресу: 123308, г. Москва, а/я 57, ООО «Орион Экспресс», а также обратившись по телефону +7 (495) 781-41-01.

VII. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Лица, виновные в нарушении норм, регулирующих защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном законодательством Российской Федерации.

ООО «Орион Экспресс»

Приложение №1
к Положению об обработке
персональных данных
в ООО «Орион Экспресс»

Сведения согласно п. 2 ч. 1 ст. 18.1. Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

Цель обработки Персональных данных	Сведения согласно п. 2 ч. 1 ст. 18.1. Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
1. обеспечение трудовых и производственных процессов с соблюдением законов и иных нормативно-правовых актов РФ	1.1. Категории и перечень, обрабатываемых ПДн: фамилия, имя, отчество; дата и год рождения; место рождения; адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания; номера телефонов (мобильного и домашнего); электронная почта; сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки; сведения о повышении квалификации и переподготовке; сведения о трудовой деятельности, трудовом стаже; сведения о номере,

	серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней; содержание и реквизиты трудового договора с работником или гражданско-правового договора с гражданином; сведения о заработной плате (банковские реквизиты счетов для расчета с Работниками, данные по окладу, надбавкам, налогам и другие сведения); сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии/снятии на (с) учет(а)); сведения о номере страхового свидетельства государственного пенсионного страхования; сведения об идентификационном номере налогоплательщика; сведения, указанные в оригиналах и копиях приказов по личному составу Компании и материалах к ним; сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) Работников Компании; материалы по аттестации и оценке Работников Компании; материалы по внутренним служебным расследованиям в отношении Работников Компании; внутрикорпоративные материалы по разбирательству и учету несчастных случаев на производстве и профессиональным заболеваниям в соответствии с Трудовым кодексом Российской Федерации, другими федеральными законами; сведения о временной нетрудоспособности работников Компании; табельный номер Работника Компании; сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения), о семейном положении, составе семьи, а также сведения о членах семьи; паспортные данные (серия, номер, кем и когда выдан). 1.2. Категории субъектов, ПДн которых обрабатываются: Работники Компании, бывшие Работники Компании 1.3. Сроки обработки и хранения ПДн: в течение срока действия трудового договора, а также в течение сроков хранения документов, предусмотренных законодательством РФ. 1.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с

	передачей по внутренней сети юридического лица, без передачи по сети Интернет. 1.5. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.
2. организации обучения	2.1. Категории и перечень, обрабатываемых ПДн: фамилия, имя, отчество; номер телефона; электронная почта; сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки; сведения о повышении квалификации и переподготовке, сведения о номере страхового свидетельства государственного пенсионного страхования, сведения об идентификационном номере налогоплательщика; паспортные данные (серия, номер, кем и когда выдан); адрес регистрации 2.2. Категории субъектов, ПДн которых обрабатываются: Работники Компании 2.3. Сроки обработки и хранения ПДн: в течение срока действия договора об организации обучения, а также в течение сроков хранения документов, предусмотренных законодательством РФ. 2.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, с передачей по сети Интернет. 2.5. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами

	информационных систем.
3. организации командировок	3.1. Категории и перечень, обрабатываемых ПДн: фамилия, имя, отчество, дата и год рождения, паспортные данные (серия, номер паспорта, кем и когда выдан) 3.2. Категории субъектов, ПДн которых обрабатываются: Работники Компании 3.3. Сроки обработки и хранения ПДн: в течение срока командировки, а также в течение сроков хранения документов, предусмотренных законодательством РФ. 3.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, с передачей по сети Интернет. 3.5. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.
4. получение ключей электронной подписи и сертификатов ключей проверки электронной подписи	4.1. Категории и перечень, обрабатываемых ПДн: фамилия, имя, отчество, дата и год рождения, паспортные данные (серия, номер, кем и когда выдан), должность, СНИЛС 4.2. Категории субъектов, ПДн которых обрабатываются: Работники Компании 4.3. Сроки обработки и хранения ПДн: в течение срока действия сертификата ключа проверки электронной подписи, а также в течение сроков хранения документов, предусмотренных законодательством РФ. 4.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, без передачи по сети Интернет. 4.5. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной

	фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.
5. оформление добровольного медицинского страхования	5.1. Категории и перечень, обрабатываемых ПДн: фамилия, имя, отчество, дата и год рождения, паспортные данные (серия, номер, кем и когда выдан); сведения о номере страхового свидетельства государственного пенсионного страхования, адрес места жительства, номер телефона, электронная почта 5.2. Категории субъектов, ПДн которых обрабатываются: Работники Компании, Родственники Работников Компании 5.3. Сроки обработки и хранения ПДн: в течение срока действия договора о добровольном медицинском страховании, а также в течение сроков хранения документов, предусмотренных законодательством РФ. 5.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, с передачей по сети Интернет. 5.5. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.
6. Реализация зарплатного проекта с целью проведения расчетов с Работниками Компании	6.1. Категории и перечень, обрабатываемых ПДн: фамилия, имя, отчество, дата и год рождения, данные паспорта (серия, номер, кем и когда выдан), адрес регистрации, адрес проживания, сведения о номере СНИЛС, табельный номер, наименование должности, дата приема, номер мобильного телефона, номер расчетного счета 6.2. Категории субъектов, ПДн которых обрабатываются: Работники Компании 6.3. Сроки обработки и хранения ПДн: в течение срока

	действия зарплатной банковской карты, а также в течение сроков хранения документов, предусмотренных законодательством РФ. 6.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, с передачей по сети Интернет. 6.5. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.
7. оформление визитных карточек	7.1. Категории и перечень, обрабатываемых ПДн: фамилия, имя, отчество, должность, номер телефона, электронная почта 7.2. Категории субъектов, ПДн которых обрабатываются: Работники Компании 7.3. Сроки обработки и хранения ПДн: в течение срока согласия на обработку ПДн, а также в течение сроков хранения документов, предусмотренных законодательством РФ. 7.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, с передачей по сети Интернет. 7.5. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.
8. оформление	8.1. Категории и перечень, обрабатываемых ПДн: фамилия,

доверенностей для выполнения Работником своих трудовых обязанностей	имя, отчество, паспортные данные (серия, номер, кем и когда выдан), место регистрации 8.2. Категории субъектов, ПДн которых обрабатываются: Работники Компании 8.3. Сроки обработки и хранения ПДн: в течение срока действия трудового договора, а также в течение сроков хранения документов, предусмотренных законодательством РФ. 8.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, без передачи по сети Интернет. 8.5. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.
9. предоставление социальных льгот Работникам	9.1. Категории и перечень, обрабатываемых ПДн: фамилия, имя, отчество, дата и год рождения; место рождения; сведения о номере страхового свидетельства государственного пенсионного страхования; место работы/учебы, сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения) 9.2. Категории субъектов, ПДн которых обрабатываются: Родственники Работников Компании 9.3. Сроки обработки и хранения ПДн: в течение срока действия трудового договора, а также в течение сроков хранения документов, предусмотренных законодательством РФ. 9.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, без передачи по сети Интернет. 9.5. Порядок уничтожения ПДн при достижении целей их

	обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.
	9.6. Категории и перечень, обрабатываемых ПДн: фамилия, имя, отчество; дата и год рождения; место рождения; адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания; паспортные данные (серия, номер паспорта, кем и когда выдан), номера телефонов (мобильного и домашнего); электронная почта; сведения о трудовой деятельности, трудовом стаже; сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней; содержание и реквизиты трудового договора с работником или гражданско-правового договора с гражданином; сведения о заработной плате (банковские реквизиты счетов для расчета с Работниками, данные по окладу, надбавкам, налогам и другие сведения); сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии/снятии на (с) учет(а)); сведения о номере страхового свидетельства государственного пенсионного страхования; сведения об идентификационном номере налогоплательщика; сведения, указанные в оригиналах и копиях приказов по личному составу Компании и материалах к ним; сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) Работников Компании; материалы по внутренним служебным расследованиям в отношении Работников Компании; внутрикорпоративные материалы по разбирательству и учету несчастных случаев на производстве и профессиональным заболеваниям в

	соответствии с Трудовым кодексом Российской Федерации, другими федеральными законами; сведения о временной нетрудоспособности работников Компании; табельный номер Работника Компании; сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения), о семейном положении, составе семьи, а также сведения о членах семьи 9.7. Категории субъектов, ПДн которых обрабатываются: Работники Компании 9.8. Сроки обработки и хранения ПДн: в течение срока действия трудового договора, а также в течение сроков хранения документов, предусмотренных законодательством РФ. 9.9. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, без передачи по сети Интернет. 9.10. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.
10. подбор кандидатов на вакантную должность; организация собеседований	10.1. Категории и перечень, обрабатываемых ПДн: фамилия, имя, отчество; дата и год рождения; место рождения; адрес места жительства; номер телефона; электронная почта; воинский учет; информация о семейном положении; сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки; сведения о повышении квалификации и переподготовке; сведения о трудовой деятельности, трудовом стаже; фотография; иные сведения, содержащиеся в резюме, сообщаемые кандидатом. 10.2. Категории субъектов, ПДн которых обрабатываются: Кандидаты на вакантную должность 10.3. Сроки обработки и хранения ПДн: до достижения цели

	обработки ПДн субъекта 10.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, без передачи по сети Интернет. 10.5. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.
11. заключение и исполнение договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных; обработка запросов, связанных с указанными договорами, информирование по заключенным договорам;	11.1. Категории и перечень, обрабатываемых ПДн: фамилия, имя, отчество; номер телефона; электронная почта; паспортные данные (серия, номер, кем и когда выдан); адрес установки приемного оборудования, марка оборудования; номер карты доступа; банковские реквизиты для перечисления денежных средств в случае их возврата 11.2. Категории субъектов, ПДн которых обрабатываются: Клиенты 11.3. Сроки обработки и хранения ПДн: в течение срока действия договора, а также в течение сроков хранения документов, предусмотренных законодательством РФ. 11.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, без передачи по сети Интернет. 11.5. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.
12. продвижение	12.1. Категории и перечень, обрабатываемых ПДн: фамилия,

товаров и услуг Компании на рынке; оценка качества услуг	имя; номер телефона; электронная почта 12.2. Категории субъектов, ПДн которых обрабатываются: Клиенты, представители контрагентов 12.3. Сроки обработки и хранения ПДн: в течение срока действия договора, а также в течение сроков хранения документов, предусмотренных законодательством РФ. 12.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, без передачи по сети Интернет. 12.5. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.
13. взаимодействие с представителями контрагентов Компании при ведении договорной работы (включая преддоговорную работу), при исполнении обязательств по договорам и соглашениям	13.1. Категории и перечень, обрабатываемых ПДн: фамилия, имя, отчество; номер телефона; электронная почта; должность 13.2. Категории субъектов, ПДн которых обрабатываются: Представители контрагентов 13.3. Сроки обработки и хранения ПДн: в течение срока действия договора, а также в течение сроков хранения документов, предусмотренных законодательством РФ. 13.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, без передачи по сети Интернет. 13.5. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.

14. проверка полномочий представителя контрагента с целью проявления Компанией должной осмотрительности	14.1. Категории и перечень, обрабатываемых ПДн: фамилия, имя, отчество; должность; адрес регистрации; паспортные данные (серия, номер, кем и когда выдан) 14.2. Категории субъектов, ПДн которых обрабатываются: Представители контрагентов 14.3. Сроки обработки и хранения ПДн: в течение срока действия договора, а также в течение сроков хранения документов, предусмотренных законодательством РФ. 14.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, без передачи по сети Интернет. 14.5. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.
15. Заключение и исполнение обязательств по договорам с лицами, выполняющими работы по гражданско-правовым договорам	15.1. Категории и перечень, обрабатываемых ПДн: фамилия, имя, отчество; номер телефона; электронная почта; сведения об идентификационном номере налогоплательщика; банковские реквизиты (в целях расчета по договорам); паспортные данные (серия, номер, кем и когда выдан); адрес регистрации, номер СНИЛС 15.2. Категории субъектов, ПДн которых обрабатываются: Лица, выполняющие работы по гражданско-правовым договорам 15.3. Сроки обработки и хранения ПДн: в течение срока действия договора, а также в течение сроков хранения документов, предусмотренных законодательством РФ 15.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, без передачи по сети Интернет. 15.5. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на

	основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.
16. Осуществление возложенных на Компанию законодательством РФ функций и обязанностей; осуществление деятельности Компании	16.1. Категории и перечень, обрабатываемых ПДн: фамилия, имя, отчество; паспортные данные (серия, номер, кем и когда выдан); дата и место рождения; сведения об идентификационном номере налогоплательщика; адрес регистрации, почтовый адрес; сведения о гражданстве; номер телефона и адрес электронной почты; доля участия в уставном капитале Компании. 16.2. Категории субъектов, ПДн которых обрабатываются: Аффилированные лица, участники Компании и их представители 16.3. Сроки обработки и хранения ПДн: в течение сроков хранения документов, предусмотренных законодательством РФ 16.4. Способы обработки и хранения ПДн: смешанная (автоматизированная и неавтоматизированная), с передачей по внутренней сети юридического лица, без передачи по сети Интернет. 16.5. Порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований: Уничтожение ПДн осуществляется комиссией, созданной на основании приказа руководителя Компании. Документальной фиксацией уничтожения ПДн субъекта является оформление соответствующего акта о прекращении обработки ПДн. После утверждения акта ПДн подлежат уничтожению встроенными средствами информационной системы администраторами информационных систем.

ООО «Орион Экспресс»

Приложение №2
к Положению об обработке
персональных данных
в ООО «Орион Экспресс»

Согласие на обработку персональных данных работника

(В соответствии с требования Федерального закона от 27.07.2006 г. № 152 ФЗ «О персональных данных»)

Я _____

(Фамилия, имя, отчество)

Паспорт: серия _____ *№* _____

выдан _____

(кем и когда выдан)

проживающий (ая) по адресу _____

_____

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», **действуя свободно, в своей воле и в своих интересах, даю согласие** на обработку моих персональных данных оператору персональных данных ООО «Орион Экспресс» (далее - Компания), ИНН 7710582109, расположенному по адресу: Российская Федерация, 107078, г. Москва вн. тер.г. муниципальный округ Басманный, Большой Харитоньевский пер., д. 24, стр. 11, помещ. 4.

Целью обработки персональных данных является:

_____

(указать цель)

_____

_____

_____

Перечень моих персональных данных, на обработку которых я даю согласие:

_____

(перечислить)

_____

_____

_____

Настоящее согласие предоставляется на сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу в случаях, прямо предусмотренных действующим законодательством РФ, обезличивание, блокирование, удаление, уничтожение персональных данных.

Я подтверждаю, что ознакомлен(-а) с перечнем операций с моими персональными данными, а также правилами обработки персональных данных, опубликованными на сайте www.orion-express.ru, осуществляемой как с использованием средств автоматизации (автоматизированная обработка, при необходимости с использованием системы видеонаблюдения), так и без использования таких средств (неавтоматизированная обработка).

Настоящее согласие действует до истечения сроков хранения соответствующей информации или документов, содержащих мои персональные данные, определяемых в соответствии с законодательством РФ или письменного уведомления субъекта о отзыве согласия, если отзыв согласия не создает нарушения действующего законодательства РФ.

Уведомление о отзыве согласия на обработку персональных данных может быть передано Компании следующими способами: путем направления по адресу: 123308, г. Москва, а/я 57, путем направления уведомления по адресу электронной почты info@orion-express.ru; иными способами.

_____ _____

Дата И.О. Фамилия

ООО «Орион Экспресс»

Приложение №3
к Положению об обработке
персональных данных
в ООО «Орион Экспресс»

Согласие на обработку персональных данных[1]

(В соответствии с требованиями Федерального закона от 27.02.2006 г. № 152 ФЗ «О персональных данных»)

Я _____

(Фамилия, имя, отчество)

Паспорт: серия _____ *№* _____

выдан _____

(кем и когда выдан)

проживающий (ая) по адресу _____

_____

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», действуя свободно, в своей воле и в своем интересе, даю согласие оператору персональных данных ООО «Орион Экспресс» (далее – Компания), ИНН 7710582109, расположенному по адресу: Российская Федерация, 107078, г. Москва вн. тер.г. муниципальный округ Басманный, Большой Харитоньевский пер., д. 24, стр. 11, помещ. 4, на обработку моих персональных данных.

Целью обработки персональных данных является:

_____

(указать цель)

_____

_____

_____

Настоящее согласие распространяется на следующую информацию, относящуюся к моим персональным данным:

_____

(перечислить)

_____

_____

_____

Настоящее согласие предоставляется на сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование,

_____

[1] Форма согласия на обработку персональных данных субъектов, отличных от Работников Компании

передачу в случаях, прямо предусмотренных действующим законодательством РФ с соблюдением требований по защите персональных данных, обезличивание, блокирование, удаление, уничтожение персональных данных.

Я подтверждаю, что ознакомлен(-а) с перечнем операций с моими персональными данными, а также правилами обработки персональных данных Компании, опубликованными на сайте www.orion-express.ru,осуществляемой как с использованием средств автоматизации (автоматизированная обработка), так и без использования таких средств (неавтоматизированная обработка). Мне также разъяснен порядок принятия решений на основании исключительно автоматизированной обработки моих персональных данных и возможных юридических последствиях такого решения. В целях исполнения договоров, заключенных между мною и Компанией, даю согласие на обработку своих персональных данных, при которой будут приниматься решения на основании исключительно автоматизированной обработки моих персональных данных.

Настоящее согласие действует до истечения сроков хранения соответствующей информации или документов, содержащих мои персональные данные, определяемых в соответствии с законодательством Российской Федерации, или направления письменного уведомления о отзыве согласия, подписанного собственноручно мною, если отзыв согласия не создает нарушения действующего законодательства РФ.

Уведомление о отзыве согласия на обработку персональных данных может быть передано Компании следующими способами: путем направления по адресу: 123308, г. Москва, а/я 57, путем направления уведомления по адресу электронной почты info@orion-express.ru; иными способами.

_____ _____

Дата И.О.Фамилия

ООО «Орион Экспресс»

Приложение №4
к Положению об обработке
персональных данных
в ООО «Орион Экспресс»

Формы запросов обращений субъектов персональных данных

Оператору персональных данных:
ООО «Орион Экспресс»
Юридический адрес:
Российская Федерация, 107078, г. Москва
вн. тер.г. муниципальный округ Басманный,
Большой Харитоньевский пер., д. 24, стр. 11,
помещ. 4
От _____
(фамилия, имя, отчество)
паспорт серии _____ номер _____
выданный _____
(дата выдачи)
_____
(место выдачи паспорта)

ЗАПРОС (ТРЕБОВАНИЕ)
на блокирование персональных данных

В соответствии с ч.1 ст.14 Федерального закона от 27.02.2006 г. № 152 ФЗ «О персональных данных» прошу произвести блокирование моих персональных данных в связи с

_____

_____
(причина блокирования)

_____ _____
(дата) (подпись)

Оператору персональных данных:
ООО «Орион Экспресс»
Юридический адрес:
Российская Федерация, 107078, г. Москва
вн. тер.г. муниципальный округ Басманный,
Большой Харитоньевский пер., д. 24, стр. 11,
помещ. 4

От _____
(фамилия, имя, отчество)

паспорт серии _____ номер _____

выданный _____
(дата выдачи)

_____
(место выдачи паспорта)

ЗАПРОС
на предоставление сведений об обработке персональных данных

В соответствии сч.1 и ч.4 ст.14 Федерального закона от 27.02.2006 г. № 152 ФЗ «О персональных данных» прошу предоставить сведения, касающиеся обработки моих персональных данных, а именно:

- подтверждение факта обработки моих персональных данных, а также правовые основания и цель такой обработки;
- способы обработки моих персональных данных;
- сведения о лицах, которые имеют доступ к моим персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки моих персональных данных, в том числе сроки их хранения;
- иные сведения, предусмотренные законодательством РФ.

_____ _____
(дата) *(подпись)*

Оператору персональных данных:
ООО «Орион Экспресс»
Юридический адрес:
Российская Федерация, 107078, г. Москва
вн. тер.г. муниципальный округ Басманный,
Большой Харитоньевский пер., д. 24, стр. 11,
помещ. 4

От _____
(фамилия, имя, отчество)

паспорт серии _____ номер _____

выданный _____
(дата выдачи)

_____
(место выдачи паспорта)

ЗАПРОС (ТРЕБОВАНИЕ)
на уничтожение персональных данных

В соответствии с ч.1 ст.14 и ч.5 ст.21 Федерального закона от 27.02.2006 г. № 152 ФЗ «О персональных данных» прошу уничтожить мои персональные данные:

_____

_____

_____

_____
(персональные данные и причина уничтожения)

_____ _____
(дата) (подпись)

Оператору персональных данных:
ООО «Орион Экспресс»
Юридический адрес:
Российская Федерация, 107078, г. Москва
вн. тер.г. муниципальный округ Басманный,
Большой Харитоньевский пер., д. 24, стр. 11,
помещ. 4

От _____
(фамилия, имя, отчество)

паспорт серии _____ номер _____

выданный _____
(дата выдачи)

_____
(место выдачи паспорта)

ЗАПРОС (ТРЕБОВАНИЕ)
на уточнение персональных данных

В соответствии с ч.1 ст.14 Федерального закона от 27.02.2006 г. № 152 ФЗ «О персональных данных» прошу внести изменения в мои персональные данные на основании сведений, содержащихся в следующих документах:

_____

_____

_____

_____
(перечень документов)

_____
(дата)

_____
(подпись)

ООО «Орион Экспресс»

Приложение №5
к Положению об обработке персональных данных
в ООО «Орион Экспресс»

ЖУРНАЛ
учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных ООО «Орион Экспресс»

Начат «___» _____ 20__ г.
Окончен «___» _____ 20__ г.
На _____ листах

Ответственный за работу с персональными данными (ПДн) _____ _____
подпись ФИО

№ п/п	Сведения о запрашивающем лице	Краткое содержание обращения	Цель запроса	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи / отказа в предоставлении информации	Подпись ответствен. работника
1	2	3	4	5	6	7