БОРЛАС
ООО «Группа Борлас»
117105, Москва, Новоданиловская наб., 4а
+7 (495) 545-59-30, info@borlas.ru
WWW.BORLAS.RU

Утверждено
Генеральный директор
ООО «Группа Борлас»
_____/Мордухович А.М./

«09» января 2018 г.

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ ООО «ГРУППА БОРЛАС»

Москва, 2018 г.

СОДЕРЖАНИЕ:

1. Общие положения 3
2. Основные понятия. Состав персональных данных работников..... 3
3. Обработка персональных данных работников 5
4. Особенности обработки персональных данных работников без использования средств автоматизации..... 9
5. Передача персональных данных 10
6. Доступ к персональным данным работников 11
7. Базовый набор мер по обеспечению доступа к персональным данным 12
8. Ответственность за нарушение норм, регулирующих обработку персональных данных..... 14

1. Общие положения

1.1. Настоящим Положением определяется порядок обращения с персональными данными работников ООО "Группа Борлас" (далее - Компания).

1.2. Упорядочение обращения с персональными данными имеет целью обеспечить соблюдение законных прав и интересов Компании и её работников в связи с необходимостью получения (сбора), систематизации (комбинирования), хранения и передачи сведений, составляющих персональные данные.

1.3. Персональные данные работника - любая информация, относящаяся к конкретному работнику (субъекту персональных данных).

1.4. Сведения о персональных данных работников относятся к числу конфиденциальных. Режим конфиденциальности в отношении персональных данных снимается:

в случае их обезличивания;

по истечении 75 лет срока их хранения;

в других случаях, предусмотренных федеральными законами.

1.5. Настоящее Положение и изменения, вносимые в него, подлежат публикации на Интернет-сайте Компании: https://borlas.ru.

2. Основные понятия. Состав персональных данных работников

2.1. Для целей настоящего Положения используются следующие основные понятия:

персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных) (п. 1 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

обработка персональных данных работника - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (п. 3 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

распространение персональных данных - действия, направленные на раскрытие персональных данных работников неопределенному кругу лиц (п. 5 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

предоставление персональных данных - действия, направленные на раскрытие персональных данных работников определенному лицу или определенному кругу лиц (п. 6 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

блокирование персональных данных - временное прекращение обработки персональных данных работников (за исключением случаев, если обработка необходима для уточнения персональных данных) (п. 7 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных работников и (или) в результате которых уничтожаются материальные носители персональных данных работников (п. 8 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному работнику (п. 9 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

информация - сведения (сообщения, данные) независимо от формы их представления;

документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2.2. Информация, представляемая работником при поступлении на работу в Компанию, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 ТК РФ лицо, поступающее на работу, предъявляет:

паспорт или иной документ, удостоверяющий личность;

трудовую книжку, за исключением случаев, когда договор заключается впервые, или работник поступает на работу на условиях совместительства, или трудовая книжка у работника отсутствует в связи с ее утратой, повреждением или по другим причинам;

страховое свидетельство обязательного пенсионного страхования;

документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;

документ об образовании и (или) квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;

справку, выданную органами МВД России, о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (при поступлении на работу, к выполнению которой в соответствии с Трудовым кодексом РФ или иным федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию) (п. п. 14, 15 Административного регламента, утвержденного Приказом МВД России от 07.11.2011 N 1121).

2.3. При оформлении работника отделом кадрового документооборота и социальных программ заполняется унифицированная форма Т-2 "Личная карточка работника", в которой отражаются следующие анкетные и биографические данные работника:

- общие сведения (Ф.И.О., дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);
- сведения о воинском учете;
- данные о приеме на работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных гарантиях;
- сведения о месте жительства и о контактных телефонах.

2.4. В отделе кадрового документооборота и социальных программ Компании создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или

сводном виде:

2.4.1. Документы, содержащие персональные данные работников:

комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;

подлинники и копии приказов (распоряжений) по кадрам;

личные дела и трудовые книжки;

дела, содержащие основания к приказу по личному составу;

дела, содержащие материалы аттестаций работников;

дела, содержащие материалы внутренних расследований;

справочно-информационные материалы (картотеки, журналы);

подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Компании, руководителям структурных подразделений;

копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

2.4.2. Документация по организации работы структурных подразделений:

положения о структурных подразделениях;

приказы, распоряжения, указания руководства Компании;

документы планирования, учета, анализа и отчетности по вопросам кадровой работы.

3. Обработка персональных данных работников

3.1. В Компании устанавливается 4-й уровень защищенности персональных данных.

3.2. Для обеспечения установленного в Компании уровня защищенности персональных данных при их обработке в информационных системах в Компании, среди прочего, выполняются:

- организация режима обеспечения безопасности помещений, в которых размещены информационные системы, в которых обрабатываются персональные данные, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей персональных данных;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз и если их применение предусмотрено федеральным законом.

Руководитель Компании утверждает документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими служебных (трудовых) обязанностей.

3.3. Компания при обработке персональных данных принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, если их применение предусмотрено федеральным законом;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) контролем принимаемых мер по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

9) иными мерами и способами, предусмотренными действующим законодательством.

3.4. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации;

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных.

3.5. При определении объема и содержания обрабатываемых персональных данных работодатель должен руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными

федеральными законами.

3.6. Руководитель Компании своим приказом назначает лицо, ответственное за организацию обработки персональных данных.

Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от Руководителя Компании и подотчетно ему.

Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

1) осуществлять внутренний контроль соблюдения Компанией и ее работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

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

3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль приема и обработки таких обращений и запросов.

3.7. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Компания принимает необходимые меры по удалению и (или) уточнению неполных и неточных данных.

3.8. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.9. Работодатель вправе обрабатывать персональные данные работников либо с их письменного согласия, либо – в случаях, предусмотренных федеральным законом, – без такого согласия. Письменное согласие работника на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- наименование и адрес оператора (Компании), получающего согласие субъекта персональных данных;

- цель обработки персональных данных;

- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

- срок, в течение которого действует согласие, а также порядок его отзыва;

- подпись работника.

3.10. Источником информации обо всех персональных данных работника является непосредственно работник. Если персональные данные возможно получить только у третьей стороны, то работник должен быть заранее в письменной форме уведомлен об этом и от него должно быть получено письменное согласие. Работодатель обязан сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о последствиях отказа работника дать письменное согласие на их получение.

3.11. Работодатель не имеет права получать и обрабатывать персональные данные работника о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

3.12. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться исключительно на автоматизированной обработке персональных данных, за исключением случаев, когда имеется согласие работника (в письменной форме) на обработку его персональных данных, а также случаев, предусмотренных федеральным законом. Компания обязана разъяснить работнику порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты своих прав и законных интересов.

Возражение, указанное во втором предложении абзаца первого настоящего пункта, рассматривается Компанией в течение тридцати дней со дня его получения, после чего работник уведомляется о результатах рассмотрения такого возражения.

3.13. Защита персональных данных работника от неправомерного их использования, утраты обеспечивается работодателем за счет его средств в порядке, установленном федеральным законом.

3.14. Работники и их представители должны быть ознакомлены под расписку с документами Компании, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

3.15. Компания и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия работника, если иное не предусмотрено федеральным законом.

3.16. В случае достижения цели обработки персональных данных Компания прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий тридцати дней с момента достижения цели обработки 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 федеральным законом.

3.17. Если Компания не вправе осуществлять обработку персональных данных без согласия работника, в случае отзыва работником согласия на обработку его персональных данных Компания прекращает их обработку и в случае, если сохранение персональных данных более не требуется для

целей обработки персональных данных, уничтожает персональные данные в срок, не превышающий тридцати дней с момента поступления указанного отзыва.

4. Особенности обработки персональных данных работников без использования средств автоматизации

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

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

4.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Компании.

4.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

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

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

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

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

4.5. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Указанные правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

4.6. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

5. Передача персональных данных

5.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

5.1.1. Не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, предусмотренных федеральным законом.

5.1.2. Предупредить лиц, получивших персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

5.1.3. Осуществлять передачу персональных данных работников в пределах Компании в соответствии с настоящим Положением.

5.1.4. Разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те

персональные данные, которые необходимы для выполнения конкретной функции.

5.1.5. Не запрашивать информацию о состоянии здоровья работника, за исключением тех

сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

5.2. Персональные данные работников обрабатываются и хранятся в отделе кадрового документооборота и социальных программ.

5.3. Персональные данные работников могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в электронном виде (посредством локальной компьютерной сети).

5.4. При получении персональных данных не от работника (за исключением случаев, если персональные данные являются общедоступными) работодатель до начала обработки таких персональных данных обязан предоставить работнику следующую информацию:

- наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные федеральными законами права субъекта персональных данных;
- источник получения персональных данных.

6. Доступ к персональным данным работников

6.1. Компания обеспечивает такой порядок хранения персональных данных, который исключает несанкционированный доступ к ним.

6.2. Все документы, содержащие персональные данные работников, такие как личные дела, картотеки, учетные журналы, хранятся в специально оборудованных шкафах или сейфах. Трудовые книжки работников хранятся в сейфе отдельно от личных дел.

6.3. Право доступа к персональным данным работников имеют:

- руководитель Компании;
- работники отдела кадрового документооборота и социальных программ;
- работники бухгалтерии;
- работники секретариата (информация о фактическом месте проживания и контактные телефоны работников);
- руководители структурных подразделений по направлению деятельности (доступ к персональным данным только работников своего подразделения).

Лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

6.4. Работник Компании имеет право:

6.4.1. Получать доступ к своим персональным данным и ознакомление с ними.

6.4.2. Требовать от работодателя уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных персональных данных.

6.4.3. Получать от работодателя сведения о:

- обрабатываемых персональных данных и источнике их получения;
- сроке обработки персональных данных, в том числе сроке их хранения;
- иные сведения в соответствии с федеральным законом.

6.4.4. Требовать извещения работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

6.4.5. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия работодателя при обработке и защите его персональных данных.

6.4.6. Иные права, предусмотренные законодательством.

7. Базовый набор мер по обеспечению безопасности персональных данных

7.1. В Компании устанавливается следующий базовый набор мер по обеспечению безопасности персональных данных:

- Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах.
- Обнаружение, идентификация и регистрация инцидентов (в т.ч. фактов несанкционированного доступа к персональным данным) и принятие мер.
- Идентификация и аутентификация пользователей являющихся работниками оператора.
- Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов.
- Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.
- Защита обратной связи при вводе аутентификационной информации.
- Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей).
- Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей.
- Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа.
- Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами.
- Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.
- Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

- Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе).
- Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.
- Регламентация и контроль использования в информационной системе технологий беспроводного доступа.
- Регламентация и контроль использования в информационной системе мобильных технических средств.
- Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).
- Определение событий безопасности, подлежащих регистрации, и сроков их хранения.
- Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.
- Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.
- Защита информации о событиях безопасности.
- Реализация антивирусной защиты.
- Обновление базы данных признаков вредоносных компьютерных программ (вирусов).
- Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.
- Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.
- Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин.
- Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены.
- Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.
- Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

7.2. Адаптированный и (или) уточненный набор мер по обеспечению безопасности персональных данных устанавливается на основе базового набора мер, приведенного в настоящем разделе, приказом руководителя Компании.

8. Ответственность за нарушение норм, регулирующих обработку персональных данных

Компания и ее работники, виновные в нарушении порядка обработки персональных данных работников, несут ответственность в соответствии с федеральным законом Российской Федерации.