Российская
Манипуляторная
Компания

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

П Р И К А З

№ 1/20 от 13.01.2023.

Об утверждении мест хранения персональных данных и лицах, ответственных за соблюдение конфиденциальности персональных данных при их хранении

В целях обеспечения конфиденциальности персональных данных в ООО «БМЗ» и в соответствии с Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных»
ПРИКАЗЫВАЮ:
1. Определить в качестве мест хранения персональных данных в архивном помещении ООО «БМЗ»
2. Ответственным за соблюдение конфиденциальности персональных данных при их хранении назначить бухгалтера ООО «БМЗ».
3. Контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор ООО «БМЗ» _____ / В.С. Полухин/

Российская
Манипуляторная
Компания

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

УТВЕРЖДАЮ

Генеральный директор ООО «БМЗ»

В.С. Полухин

13.01.2023

Правила обработки персональных данных без использования средств автоматизации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Обработка персональных данных считается осуществленной без использования средств автоматизации (неавтоматизированной), если обработка персональных данных осуществляется без помощи средств вычислительной техники.

1.2. Категории обрабатываемых персональных данных и категории субъектов персональных данных, а также цели обработки персональных данных указаны в утвержденном положении о защите и обработке персональных данных.

1.3. В ООО «БМЗ» не обрабатываются биометрические и специальные категории персональных данных.

1.4. Обработка персональных данных без использования средств автоматизации осуществляется на законной и справедливой основе. Обработка персональных данных без использования средств автоматизации не может быть использована ООО «БМЗ» или его работниками в целях причинения материального и морального вреда субъектам персональных данных, затруднения реализации их прав и свобод.

1.5. Настоящие правила обработки персональных данных без использования средств автоматизации (далее – Правила) разработаны и утверждены в целях обеспечения безопасности персональных данных, обрабатываемых в ООО «БМЗ» без использования средств автоматизации, и исполнения требований Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

1.6. Настоящие Правила являются внутренним локальным актом ООО «БМЗ», вступают в силу с момента их утверждения генеральным директором ООО «БМЗ» и действуют бессрочно до их замены новым документом.

1.7. Все работники ООО «БМЗ», допущенные к неавтоматизированной обработке персональных данных, должны быть ознакомлены с настоящими Правилами под роспись.

1.8. Ответственность за актуализацию настоящих Правил и контроль над выполнением настоящих Правил возлагаются на назначенного Генеральным директором ООО «БМЗ» ответственного за организацию обработки персональных данных.

2. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

2.1. В ООО «БМЗ» без использования средств автоматизации обрабатываются персональные данные работников, соискателей и контрагентов. Обрабатываемые категории персональных данных для различных категорий субъектов установлены в разделе 2.2 положения о защите и обработке персональных данных, утвержденного в ООО «БМЗ».

2.2. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются 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).

2.3. 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.

2.4. К обработке персональных данных без использования средств автоматизации допущены только те работники, которые указаны в утвержденных в ООО «БМЗ» перечнях лиц, допущенных к обработке персональных данных.

2.5. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, подписывают соглашение о неразглашении персональных данных.

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

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки персональных данных;
- 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;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

2.7. Журналы (реестры, книги), содержащие персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию ООО «БМЗ», не ведутся.

2.8. 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:

- 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;
- 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.

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

2.9. Для уничтожения персональных данных на материальных носителях в ООО «БМЗ» утвержден состав комиссии по уничтожению персональных данных, а также утверждена форма уничтожения персональных данных.

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

3. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

3.1. С целью обеспечения безопасности персональных данных при их обработке без использования средств автоматизации приказом Генерального директора ООО «БМЗ» определены места хранения персональных данных, а также назначены ответственные за обеспечение конфиденциальности персональных данных при их хранении.

3.2. Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях (разные места хранения для разных категорий субъектов персональных данных).

3.3. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, определены в Положении о защите и обработке персональных данных в ООО «БМЗ»

Российская
Манипуляторная
Компания

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

П Р И К А З

№ 1/21 от 13.01.2023.

О порядке хранения и эксплуатации средств криптографической защиты информации (СКЗИ) в ООО «БМЗ»

В целях исполнения нормативных документов

- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности (утв. приказом ФСБ России от 10.07.2014 № 378);
- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (утв. приказом ФСБ России от 09.02.2005 № 66);
- Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (утв. приказом ФАПСИ от 13.06.2001 № 152).

ПРИКАЗЫВАЮ:

1. Ответственным за хранение и эксплуатацию СКЗИ (органом криптографической защиты – ОКЗ) в ООО «БМЗ» назначить Главного бухгалтера.
2. К работе с СКЗИ допускать только пользователей (далее – Пользователи), прошедших предварительное обучение работе с СКЗИ согласно утвержденному перечню лиц (Приложение № 1).
3. Пользователям и ОКЗ в своей работе, связанной с обеспечением безопасности СКЗИ, ключевых документов, ключевых носителей и эксплуатационной документации к СКЗИ руководствоваться утвержденной инструкцией по обеспечению безопасности эксплуатации СКЗИ (Приложение № 2).
4. Поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых документов вести в Журнале по форме, утвержденной в Приложении № 5 к настоящему Приказу.
5. Назначить комиссию по уничтожению криптографических ключей и ключевых носителей в составе:

Генеральный директор – председатель комиссии;
Главный бухгалтер – член комиссии;
Бухгалтер – член комиссии.

Российская
Манипуляторная
Компания

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

Комиссии по уничтожению криптографических ключей и ключевых носителей руководствоваться разделом 5 инструкции по обеспечению безопасности эксплуатации СКЗИ (Приложение № 2), формой акта уничтожения (Приложение № 3) и действующим законодательством в сфере обеспечения безопасности информации с использованием криптографических средств защиты информации.

6. Утвердить схему организации криптографической защиты конфиденциальной информации (Приложение №4).

7. Контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор ООО «БМЗ» _____ / В.С. Полухин/

Российская
Манипуляторная
Компания

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

П Р И К А З

№ 1/22 от 13.01.2023.

**О назначении комиссии по уничтожению документов,
содержащих персональные данные**

В целях исполнения требований федерального закона №152-ФЗ «О персональных данных» в части, касающейся уничтожения документов, содержащих персональные данные по истечении срока обработки персональных данных,

ПРИКАЗЫВАЮ:

1) создать комиссию в ООО «БМЗ» по уничтожению документов, содержащих персональные данные работников, соискателей и контрагентов ООО «БМЗ» в составе:

Председатель комиссии:

Генеральный директор

Члены комиссии:

Главный бухгалтер

Бухгалтер

2) комиссии в своей работе руководствоваться положениями федерального закона №152-ФЗ «О персональных данных»;

3) утвердить прилагаемую форму акта об уничтожении документов, содержащих персональные данные;

4) контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор ООО «БМЗ» _____ / В.С. Полухин/

Российская
Манипуляторная
Компания

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

УТВЕРЖДАЮ

Генеральный директор ООО «БМЗ»

В.С. Полухин

13.01.2023

ПОЛОЖЕНИЕ
О ЗАЩИТЕ И ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ООО «БМЗ»

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

СОДЕРЖАНИЕ

Российская Манипуляторная Компания

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение и область действия документа

Настоящее Положение об обработке персональных данных в ООО «БМЗ» (далее — Положение) определяет порядок сбора, хранения, передачи, использования, уничтожения и любых других видов обработки персональных данных субъектов персональных данных в ООО «БМЗ».

Настоящее Положение разработано в соответствии с федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — Закон), постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Трудовым кодексом РФ.

Цель данного Положения – определение порядка обработки персональных данных субъектов персональных данных в ООО «БМЗ» (далее — Организация).

Юридические и физические лица, в соответствии со своими полномочиями владеющие, получающие и использующие информацию о субъектах персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную, предусмотренную законодательством Российской Федерации, ответственность за нарушение правил обработки и защиты этой информации.

Настоящее Положение вступает в силу с момента его утверждения Генеральный директор ООО «БМЗ» Организации и действует бессрочно до замены его новым Положением.

Все изменения в Положение вносятся приказом Генерального директора Организации.

Все сотрудники Организации, имеющие доступ к персональным данным субъектов персональных данных, в обязательном порядке должны быть ознакомлены с настоящим Положением под роспись для последующего его исполнения.

ОСНОВНЫЕ ПОНЯТИЯ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.2 Термины и определения

Автоматизированная обработка персональных данных - обработка персональных данных с использованием средств вычислительной техники.

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

Атака – целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой криптосредством информации или с целью создания условий для этого.

Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

Безопасность объекта – состояние защищенности объекта от внешних и внутренних угроз.

Безопасность информации – состояние защищённости информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации.

Блокирование информации – временное прекращение сбора, систематизации, накопления, использования, распространения, информации, в том числе её передачи.

Доступ к информации – возможность получения информации и ее использования.

Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

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

Информация – сведения (сообщения, данные) независимо от формы их представления.

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

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

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

Контролируемая зона - это пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Модель угроз – перечень возможных угроз информации.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

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

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

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

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

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

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

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

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

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

Уничтожение информации – действия, в результате которого невозможно восстановить содержание информации в информационной системе или в результате которых уничтожаются материальные носители информации.

Уполномоченное оператором лицо – лицо, которому на основании договора оператор поручает обработку персональных данных.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

1.3 Определение перечня персональных данных, обрабатываемых в ООО «БМЗ»

В Организации обрабатываются персональные данные следующих категорий субъектов персональных данных:

Персональные данные работников

Цели обработки персональных данных работников:

1) ведение кадрового учета в соответствии с Трудовым кодексом Российской Федерации;

2) начисление заработной платы и премиального вознаграждения;

3) организации системы доступа в помещения ООО «БМЗ»;

4) подготовка регламентированной отчетности в государственные контрольные органы (ФНС, ПФР, ФСС и другие).

В ООО «БМЗ» как с помощью средств автоматизации, так и без использования таких средств обрабатываются следующие категории персональных данных сотрудников:

фамилия, имя, отчество; дата и место рождения; гражданство; семейное положение; состав семьи; паспортные данные; сведения об образовании; сведения о трудовом стаже; занимаемая должность; сведения о воинской обязанности; адрес регистрации и фактического места жительства; контактные телефоны; сведения о доходах; данные трудового договора; подлинники и копии приказов по личному составу; дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям; анкеты; результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей (без диагноза и других медицинских данных); фотография; индивидуальный номер налогоплательщика; номер страхового свидетельства обязательного пенсионного страхования; сведения об отпусках; сведения о социальных льготах и гарантиях; код карты доступа в помещения; номер карты доступа в помещения; уровень доступа в помещения; время действия карты доступа в помещения; дата выдачи карты доступа в помещения; тип карты доступа в помещения.

Персональные данные соискателей на вакантные должности

Цели обработки персональных данных соискателей:

1) трудоустройство на вакантные должности ООО «БМЗ».

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

В ООО «БМЗ» как с помощью средств автоматизации, так и без использования таких средств обрабатываются следующие категории персональных данных соискателей:

фамилия, имя, отчество; дата рождения; место рождения; гражданство; пол; сведения о воинском учете; сведения об образовании; сведения о трудовом стаже; другие данные, указанные соискателем самостоятельно в резюме.

Персональные данные контрагентов

Цели обработки персональных данных контрагентов:

1) покупка ООО «БМЗ» техники или запасных частей у контрагента;

2) оказание контрагенту услуг по ремонту техники;

3) оказание контрагенту услуг по продаже техники.

В ООО «БМЗ» как с помощью средств автоматизации, так и без использования таких средств обрабатываются следующие категории персональных данных контрагентов:

фамилия, имя, отчество; ОКОПФ; паспортные данные; адрес регистрации; контактные данные; адрес электронной почты; данные о счетах и договорах; банковские реквизиты счета контрагента.

Принципы обработки персональных данных

1.4 Общие принципы обработки

Обработка персональных данных должна осуществляться на основе принципа соответствия объема и характера обрабатываемых персональных данных, а также способов обработки персональных данных заявленным целям обработки персональных данных.

Сбор, накопление, хранение, изменение, использование и распространение, а также другие действия, понимаемые под обработкой персональных данных, могут осуществляться только при условии письменного согласия физического лица, за исключением случаев, предусмотренных Законом.

Обработка персональных данных обрабатывается как с помощью средств автоматизации, так и без использования таких средств.

Правила обработки и защиты персональных данных без использования средств автоматизации установлены в соответствующем внутреннем документе ООО «БМЗ».

Правила обработки персональных данных в информационной системе персональных данных установлены в Инструкции администратора информационной безопасности и в Инструкции пользователя информационной системы персональных данных.

1.5 Порядок сбора и хранения персональных данных

При сборе персональных данных Организация обязана предоставить физическому лицу (субъекту персональных данных) по его запросу информацию о целях, способах обработки персональных данных, сведения о лицах, имеющих доступ к персональным данным, перечень обрабатываемых персональных данных и источник их получения, сведения о сроках обработки и хранения персональных данных.

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

Информация, представляемая работником при приеме на работу, должна иметь документальное оформление. При заключении трудового договора в соответствии со статьей 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;
- дополнительные документы - в случаях предусмотренных федеральными законами, указами Президента РФ или постановлениями Правительства РФ.

В структурных подразделениях по управлению персоналом предприятия создаются, обрабатываются и хранятся следующие документы, содержащие персональные данные работников:

а) Карточка ф. Т-2, в которой отражаются следующие анкетные и биографические данные работника, которые относятся к персональным данным:

общие сведения (ФИО работника, дата рождения, место рождения, пол, гражданство, знание иностранного языка, образование, профессия, общий трудовой стаж, состояние в браке, паспортные данные, адрес места жительства, дата регистрации по месту жительства, номер телефона);

- сведения о воинском учете;
- данные о приеме на работу.

В дальнейшем в карточку ф. Т-2 вносятся:

- сведения о переводах на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;

- сведения об отпусках;
- сведения о социальных льготах и гарантиях.

б) Анкета, которая заполняется работником при приеме на работу (содержатся анкетные и биографические данные работника).

в) Трудовой договор (содержит сведения о должности работника, заработной плате, месте работы, рабочем месте, а также иные персональные данные работника).

г) Подлинники и копии приказов по личному составу и основания к ним (содержат информацию о приеме, переводе, увольнении и иных событиях, относящихся к трудовой деятельности работника).

д) Трудовая книжка или ее копия (содержит сведения о трудовом стаже, предыдущих местах работы).

е) Копии свидетельств о заключении брака, рождении детей (необходимы работодателю для предоставления работнику определенных льгот, предусмотренных трудовым и налоговым законодательством).

ж) Справка о доходах с предыдущего места работы (необходима работодателю для предоставления работнику определенных льгот и компенсаций в соответствии с налоговым законодательством).

з) Справка о сумме заработной платы, иных выплат и вознаграждений за 2 последние календарные года для начисления пособия по временной нетрудоспособности.

и) Копии документов об образовании (подтверждают квалификацию работника, обосновывают занятие определенной должности).

к) При необходимости иные документы (материалы служебных расследований, подлинники и копии отчетных, аналитических и справочных материалов), содержащие персональные данные работников.

Персональные данные соискателей на вакантные должности попадают в Организацию через специализированные веб-сайты (электронные биржи труда) или направляются соискателями непосредственно на электронную почту Организации. В случае приглашения соискателя на собеседование, данные в резюме могут подтверждаться документально. Копии подтверждающих документов могут храниться в Организации, но не дольше чем до достижения цели их обработки, то есть до замещения вакантной должности.

Персональные данные контрагентов поступают в Организацию при заключении договора, подтверждаются оригиналами документов и хранятся в течение исполнения договорных обязательств.

1.6 Процедура получения персональных данных работников

При заключении трудового договора работник обязан предоставить следующие документы, содержащие его персональные данные:

– действующий российский паспорт или иной документ, удостоверяющий личность;

– трудовую книжку;

– страховое свидетельство государственного пенсионного страхования;

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

– документы воинского учета (военный билет);
– документы об образовании;
– водительское удостоверение (в зависимости от должности);
– идентификационный номер налогоплательщика (при наличии).

Если трудовой договор с работником заключается впервые, трудовая книжка и страховое свидетельство государственного пенсионного страхования оформляются Организацией. В некоторых случаях, в зависимости от характера выполнения работы и конкретных должностных обязанностей, работник должен предоставить дополнительные документы, такие как:

– заграничный паспорт;
– медицинскую справку о стоянии здоровья;
– справку о доходах.

Этот список не ограничивается вышеперечисленными документами и может включать иные документы, содержащие персональные данные работника и необходимые Организации для выполнения ею своих обязательств как по отношению к работнику, так и к третьей стороне. В случае необходимости Организация вправе обратиться к работнику с просьбой о предоставлении документов, содержащих его персональные данные.

Все персональные данные работника следует получать непосредственно от него самого.

Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие на получение его персональных данных у третьей стороны. Организация должна сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

Работник при изменении персональных данных письменно уведомляет работодателя о таких изменениях в срок, не превышающий трех рабочих дней.

В соответствии со статьей 86 главы 14 Трудового кодекса Российской Федерации в целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника должны соблюдать следующие общие требования:

- обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- при определении объема и содержания обрабатываемых персональных данных работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом РФ и иными федеральными законами;
- защита персональных данных работника от неправомерного их использования или утраты обеспечивается работодателем за счет его средств в порядке,

установленном Трудовым кодексом РФ и Федеральным законом РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;

- работники и их представители должны быть ознакомлены под роспись с документами предприятия, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

1.7 Передача персональных данных третьим лицам

Передача персональных данных третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных федеральным законом, не допускается. Данное ограничение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами.

Передача персональных данных субъекта в коммерческих целях без его письменного согласия исключается. Обработка персональных данных субъекта в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

Лица, получившие доступ к персональным данным субъекта, должны быть предупреждены о том, что эти данные могут быть использованы лишь в целях, для которых они переданы, и обязаны соблюдать это правило. Лица, получившие персональные данные, обязаны соблюдать режим конфиденциальности.

Передача или получение персональных данных осуществляются в соответствии с утвержденными Правилами рассмотрения запросов субъектов персональных данных или их представителей.

Персональные данные соискателей и контрагентов третьим лицам не передаются.

Персональные данные работников передаются в государственные контролирующие органы в соответствии с федеральными законами (ФНС, ФСС, ПФР и др.), а также в рамках зарплатного проекта в банк. Передача персональных данных в финансовую организацию производится с информированного и осознанного согласия работника. В пункте Х.Х соглашения № ХХХХ от ДД.ММ.ГГГГ между ООО «БМЗ» и банка предусмотрена обязанность третьего лица обеспечения конфиденциальности полученной от Организации информации, в том числе и персональных данных.

1.8 Трансграничная передача персональных данных

Трансграничная передача персональных данных Организацией не осуществляется.

Все технические средства обработки персональных данных (рабочие станции и сервера) находятся в пределах Российской Федерации.

1.9 Порядок уничтожения и блокирования персональных данных

Организация обязана прекратить обработку персональных данных и уничтожить их после достижения цели обработки или в случае отзыва субъектом персональных данных

согласия на обработку, за исключением случаев, когда уничтожение противоречит федеральному законодательству, а также уведомить о своих действиях субъекта персональных данных и (или) уполномоченный орган. Во всех случаях предусмотрен срок уничтожения персональных данных – три рабочих дня.

В целях оперативной организации уничтожения персональных данных на бумажных носителях приказом Генерального директора Организации назначена комиссия по уничтожению персональных данных, а также утверждена форма акта уничтожения персональных данных.

Персональные данные, обрабатываемые в информационной системе персональных данных, удаляются путем стирания записи в базах данных администратором информационной безопасности Организации по запросу субъекта или при достижении целей обработки персональных данных.

Временное прекращение операций по обработке персональных данных (блокирование) должно возникать по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

1.10 Защита персональных данных

При обработке персональных данных Организация принимает организационные и технические меры для защиты персональных данных от неправомерных действий в соответствии с требованиями, устанавливаемыми Правительством РФ.

Защита персональных данных при неавтоматизированной их обработке регламентируется внутренним документом «Правила обработки персональных данных без использования средств автоматизации».

Защита персональных данных при их обработке в информационной системе персональных данных (далее - ИСПДн) регламентирована Инструкцией администратора безопасности ИСПДн, Инструкцией пользователя ИСПДн и другими внутренними документами Организации по защите информации.

Приказом Генерального директора Организации назначена группа реагирования на инциденты информационной безопасности.

В Организации разработана Модель угроз ИСПДн и Модель нарушителя. Проведена классификация ИСПДн. Для ИСПДн сформировано Техническое задание на систему защиты информации, в котором описаны все организационные и технические меры, которые необходимо осуществить для нейтрализации актуальных угроз и выполнения требований действующего законодательства по защите персональных данных установленного уровня защищенности.

В Организации проведена внутренняя оценка эффективности принятых мер по защите персональных данных, подтвердившая в целом удовлетворительное состояние системы защиты персональных данных.

1.11 Согласие на обработку персональных данных

С соискателей согласия на обработку персональных данных берутся только в случае приглашения соискателя на собеседование в офис Организации.

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

Размещая свое резюме на электронных биржах труда или присылая резюме на электронную почту Организации, соискатель автоматически дает свое согласие на обработку его персональных данных.

С контрагентов согласия на обработку персональных данных не берутся, поскольку обработка их персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных. В соответствии с пп. 5, п. 1 статьи 6 Федерального закона № 152-ФЗ «О персональных данных» согласие на обработку персональных данных в таких случаях не требуется.

Со всех работников Организации собирается согласие на обработку их персональных данных. Несмотря на то, что обработка персональных данных производится в основном в соответствии с Трудовым Кодексом Российской Федерации, персональные данные работников в рамках зарплатного проекта передаются третьему лицу (банк). В соответствии с п. 3 статьи 6 Федерального закона № 152-ФЗ «О персональных данных» такая передача персональных данных возможна только с согласия субъекта персональных данных.

ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

1.12 Организация доступа работников к персональным данным субъектов

Должностные лица Организации должны иметь доступ только к тем персональным данным, которые необходимы им для выполнения своих функциональных обязанностей.

В Организации разработана и утверждена разрешительная система допуска к персональным данным (Положение о разграничении прав доступа к персональным данным). Круг лиц, допущенных к обработке персональных данных, определяет руководство Организации на основании данных, представленных руководителями подразделений, в которых ведется обработка персональных данных. Данный Перечень утверждается Генеральным директором Организации.

Должностные лица Организации допускаются к обработке персональных данных после ознакомления с настоящим Положением, инструкцией пользователя ИСПДн а также с иной организационно-распорядительной документацией Организации по защите персональных данных.

Должностные лица Организации перед началом обработки персональных данных подписывают соглашение о неразглашении персональных данных.

Доступ должностных лиц к обработке персональных данных осуществляется в соответствии с Перечнем лиц, должностей, служб и процессов, допущенных к работе с персональными данными.

В случае обнаружения нарушений правил обработки персональных данных в Организации руководство Организации и/или администратор безопасности информации и/или ответственный за организацию обработки персональных данных обязаны приостановить предоставление персональных данных пользователям до выявления и устранения причин нарушений.

Работники Организации имеют право на свободный бесплатный доступ к своим персональным данным, а также на получение копий любой записи о своих персональных данных, обрабатываемых в Организации.

Лица, не имеющие доступа к персональным данным в соответствии с Перечнем подразделений и сотрудников, допущенных к работе с персональными данными, могут быть допущены к ним на основании приказа, подписанного Генеральным директором Организации либо руководителем подразделения данного лица.

1.13 Организация доступа субъекту персональных данных к его персональным данным

Организация, обрабатывающая персональные данные, должна обеспечивать бесплатный доступ субъекта к персональным данным, ему соответствующим, за исключением случаев получения персональных данных в результате оперативно-розыскной деятельности, а также других случаев, предусмотренных федеральным законодательством.

Для получения доступа к своим персональным данным субъекту необходимо направить в Организацию запрос, содержащий паспортные данные субъекта персональных данных, в бумажной или электронной форме, подписанные собственноручно или квалифицированной электронной подписью.

Работники Организации должны предоставить персональные данные субъекту в доступной форме, в них не должны содержаться персональные данные, относящиеся к другим субъектам.

В случае если персональные данные субъекта являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, Организация обязана удовлетворить требование субъекта по устранению нарушений обработки персональных данных.

С целью организации своевременной обработки запросов и обращений субъектов персональных данных в Организации разработан и утвержден документ «Правила рассмотрения запросов субъектов персональных данных или их представителей».

Права и обязанности ООО «БМЗ»

1.14 Права и обязанности Организации

Организация имеет право осуществлять обработку персональных данных в законных и обоснованных целях, в том числе предоставлять персональные данные третьим лицам, если на это дано информированное согласие субъекта персональных данных или если это предусмотрено действующим законодательством.

В случае выявления недостоверных персональных данных или неправомерных действий с ними Организации при обращении или по запросу субъекта персональных данных или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных, Организация обязана устранить допущенные нарушения или, в случае невозможности устранения, уничтожить персональные данные, а также уведомить о своих действиях субъекта персональных данных или уполномоченный орган.

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

Должностные лица Организации, в обязанность которых входит обработка запросов и обращений субъектов персональных данных, обязаны обеспечить каждому субъекту возможность ознакомления с документами и материалами, содержащими их персональные данные, если иное не предусмотрено законом, в соответствии с Правилами рассмотрения запросов субъектов персональных данных.

В случае предоставления субъектом неполных, устаревших, недостоверных или незаконно полученных персональных данных Организация обязана внести необходимые изменения, уничтожить или блокировать их, а также уведомить о своих действиях субъекта персональных данных.

Организация обязуется не принимать на основании исключительно автоматизированной обработки решения, порождающие юридические последствия в отношении субъектов персональных данных или иным образом затрагивающие их права и законные интересы.

По запросу уполномоченного органа по защите прав субъектов персональных данных Организация обязана предоставить ему необходимую информацию.

ПРАВА И ОБЯЗАННОСТИ РАБОТНИКов ООО «БМЗ»

1.15 Общие положения

Работники, допущенные к обработке персональных данных, обязаны ознакомиться с документами Организации, которые устанавливают порядок обработки персональных данных в Организации, и подписать лист ознакомления с ними, а также подписать соглашение о неразглашении персональных данных, полученных в ходе исполнения своих должностных обязанностей.

1.16 Права работника

В целях защиты персональных данных, хранящихся в Организации, работник имеет право:

– требовать исключения или исправления неверных или неполных персональных данных;

– на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

– определять своих представителей для защиты своих персональных данных;

– на сохранение и защиту своей личной и семейной тайны;

– на обжалование в суде любых неправомерных действий или бездействия Организации при обработке и защите его персональных данных.

В целях защиты персональных данных, хранящихся в Организации, работник, осуществляющий обработку персональных данных, имеет право:

– получать и вводить информацию в соответствии с его полномочиями;

– требовать оповещения Организацией субъекта персональных данных обо всех произведенных в них исключениях, исправлениях или дополнениях.

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

1.17 Обязанности работника

В части своих персональных данных:

– передавать Организации достоверные документы, содержащие персональные данные, состав которых установлен Трудовым кодексом РФ;

– не предоставлять неверные персональные данные, а в случае изменений в персональных данных или обнаружения ошибок или неточностей в них (фамилия, место жительства и т.д.), незамедлительно сообщить об этом в Организацию.

В части обработки персональных данных субъекта:

– соблюдать режим конфиденциальности;

– не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия;

– не сообщать персональные данные субъекта третьей стороне без письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральным законом;

– разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;

– не запрашивать дополнительную информацию, содержащую персональные данные, за исключением тех сведений, которые необходимы для достижения целей обработки персональных данных.

Права субъектов персональных данных

1.18 Получение сведений об Организации

Субъект персональных данных имеет право на получение сведений об Организации, о месте ее нахождения, о наличии у Организации персональных данных, относящихся к нему, а также на ознакомление с такими персональными данными. Субъект персональных данных вправе требовать от Организации уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

1.19 Доступ к своим персональным данным

Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю Организацией при обращении либо при получении запроса субъекта персональных данных или его законного представителя.

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных Организацией, а также цель такой обработки;

– способы обработки персональных данных, применяемые Организацией;

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– сроки обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

Если субъект персональных данных считает, что Организация осуществляет обработку его персональных данных с нарушением требований федерального законодательства или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Организации в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

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

1.20 Ограничение прав субъектов персональных данных

Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:

1) обработка персональных данных, в том числе персональных данных, полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) предоставление персональных данных нарушает конституционные права и свободы других лиц.

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.21 Общие положения

Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность за нарушение режима защиты, обработки и порядка использования этой информации.

Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъекта персональных данных, действующего на основании законодательства о персональных данных.

1.22 Персональная ответственность должностных лиц ООО «БМЗ»

Должностные лица Организации, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность, предусмотренную федеральным законодательством.

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

Руководитель подразделения, разрешивший доступ должностному лицу к персональным данным несет персональную ответственность за данное решение.

Должностные лица Организации, получающие доступ к персональным данным несут персональную ответственность за обеспечение конфиденциальности предоставленной им информации. Кроме того, должностные лица Организации, получающие для работы документы, содержащие персональные данные, несут персональную ответственность за их сохранность.

В случае, когда нарушение конфиденциальности, целостности или доступности персональных данных повлекло за собой какие-либо финансовые потери для Организации, виновные должностные лица обязаны возместить причиненный ущерб.

Российская
Манипуляторная
Компания

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

П Р И К А З

№ 1/23 от 13.01.2023.

О назначении группы реагирования на инциденты информационной безопасности и о правилах регистрации инцидентов информационной безопасности и реагирования на них

В целях исполнения требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных Приказом ФСТЭК России № 17 от 11.02.2013 в части регистрации событий безопасности

ПРИКАЗЫВАЮ:

1. Назначить внутреннюю группу по реагированию на инциденты информационной безопасности (далее – ГРИИБ) в составе:

Генеральный директор – председатель комиссии;

Главный бухгалтер – член комиссии;

Бухгалтер – член комиссии.

2. Утвердить прилагаемую, разработанную в соответствии с ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», инструкцию по реагированию на инциденты информационной безопасности.

3. ГРИИБ в своей работе руководствоваться инструкцией по реагированию на инциденты информационной безопасности, руководящими документами ФСТЭК России и ФСБ России, государственными стандартами в области информационной безопасности и общедоступными источниками об угрозах и уязвимостях информационных систем.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор ООО «БМЗ» _____ / В.С. Полухин/

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

УТВЕРЖДАЮ

Генеральный директор ООО «БМЗ»

В.С. Полухин

13.01.2023

Инструкция по реагированию на инциденты информационной безопасности в ООО «БМЗ»

1 ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Политики информационной безопасности и меры по защите информации в ГИС не могут полностью гарантировать защиту информации, информационных систем, сервисов или сетей. Всегда существует вероятность, что после внедрения системы защиты информации останутся слабые места, которые могут сделать обеспечение информационной безопасности неэффективным, и, следовательно, инциденты информационной безопасности – возможными. Инциденты информационной безопасности могут оказывать прямое или косвенное негативное воздействие на деятельность ООО «БМЗ». Также неизбежно выявление новых, ранее не идентифицированных угроз безопасности информации. Исходя из вышесказанного, важно применять структурный подход к:

- обнаружению, оповещению об инцидентах безопасности и их оценке;
- реагированию на инциденты информационной безопасности, включая активизацию соответствующих защитных мер для предотвращения, уменьшения последствий и (или) восстановления после наступления негативных последствий вследствие инцидента безопасности информации;
- извлечению уроков из инцидентов информационной безопасности, совершенствованию системы защиты информации, введению превентивных защитных мер и улучшению общего подхода к менеджменту инцидентов информационной безопасности.

2.2. Регистрация событий безопасности, выявление инцидентов безопасности информации и реагирование на них производится, в том числе, с целью выполнения требований Приказа ФСТЭК № 17 от 11.02.2013 с индексами: РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.5, РСБ.6, РСБ.7.

2.3. Для реагирования на инциденты информационной безопасности создается группа реагирования на инциденты информационной безопасности (далее – ГРИИБ).

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

2.4. Важным членом ГРИИБ является Администратор безопасности информации (далее – Администратор), назначаемый приказом руководителя ООО «БМЗ». Он осуществляет централизованный мониторинг событий безопасности в соответствии с Инструкцией администратору безопасности.

2.5. Инцидентом информационной безопасности (далее - инцидент ИБ) является событие, нарушающее одно из свойств защищаемой информации (целостность, доступность или конфиденциальность) или несколько таких свойств одновременно.

3. РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ

3.1. События безопасности, подлежащими регистрации, являются записи в журналах операционных систем, прикладного программного обеспечения и средств защиты информации (электронные журналы сообщений). К событиям безопасности относятся следующие виды записей в таких системных журналах.

3.2. Информация о событиях безопасности информации является защищаемой информацией и к ней применяются те же, утвержденные правила и политики по защите информации, что и к другой защищаемой конфиденциальной информации в ООО «БМЗ».

3.3. Далеко не все события безопасности информации являются инцидентами безопасности информации. Инцидентами безопасности являются только запрещенные в ГИС действия, с которыми может быть связано создание угрозы информационной безопасности.

3.4. Информация о событиях безопасности также может поступать Администратору безопасности от сотрудников ООО «БМЗ», заметивших аномальную активность в информационной системе. Информацией о событиях безопасности также являются сведения о потере, краже или компрометации машинных и других носителей информации.

3.5. Администратор анализирует электронные журналы сообщений и принимает решение, является ли событие безопасности инцидентом информационной безопасности.

3.6. По степени возможного ущерба информационной системе и ООО «БМЗ» инциденты информационной безопасности можно условно разделить на незначительные и значительные.

3.7. Незначительными признаются инциденты информационной безопасности, соответствующие одному или нескольким критериям:

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

- инцидент был быстро обнаружен и локализован, значительных последствий в результате инцидента не произошло;
- инцидент затронул небольшое количество сотрудников ООО «БМЗ»;
- инцидент не требует существенных усилий и затрат на восстановление работоспособности информационной системы или ее частей;
- в результате инцидента не была нарушена конфиденциальность, целостность и доступность больших массивов защищаемой информации (например, всей базы данных), нарушена безопасность только небольшого фрагмента информации (одной или нескольких записей базы данных);
- инцидент не требует концептуального пересмотра политик информационной безопасности в ООО «БМЗ»;
- в результате инцидента организации нанесен минимальный ущерб или не нанесено никакого ущерба;
- инцидент не вызвал долгосрочного простоя информационной системы и не нарушил бизнес-процессы и технологические процессы обработки информации.

3.8. Значительными признаются все инциденты информационной безопасности, которые не могут быть признаны незначительным в соответствии с пунктом 2.7 данной Инструкции.

4. РЕАГИРОВАНИЕ НА ИНЦИДЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УСТРАНЕНИЕ ПОСЛЕДСТВИЙ И ПРИЧИН ИНЦИДЕНТА

4.1. В случае обнаружения незначительных инцидентов, Администратор самостоятельно принимает меры по устранению последствий инцидента информационной безопасности.

4.2. В случае обнаружения значительных инцидентов, Администратор созывает ГРИИБ, которая оценивает инцидент и реагирует на него наиболее целесообразным и результативным способом.

4.3. После устранения последствий инцидента, ГРИИБ делаются соответствующие выводы (оформляемые в виде акта) и вносятся предложения по совершенствованию технических и организационных аспектов защиты информации с целью предотвращения подобных инцидентов в будущем.

4.4. Процесс реагирования на инцидент информационной безопасности и восстановление ущерба, нанесенного, может состоять из следующих этапов:

- обнаружение и оповещение о возникновении событий ИБ (человеком или автоматическими средствами);
- сбор информации, связанной с событиями информационной безопасности и оценка этой информации с целью определения, какие события можно отнести к категории инцидентов ИБ;
- незамедлительное реагирование на инцидент ИБ;

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

- локализация АРМ или сегмента сети, на который распространились негативные последствия инцидента;
- при необходимости - привлечение специалистов сторонних организаций для получения качественных консультаций;
- выполнение мер по нейтрализации факторов, вызвавших инцидент ИБ;
- восстановление ущерба, вызванного инцидентом ИБ;
- регистрация всех действий и решений для последующего анализа;
- правовая оценка инцидента ИБ;
- при необходимости и при наличии правовых оснований, обращение в правоохранительные органы;
- принятия мер для предотвращения подобных инцидентов в будущем.

5. РАССЛЕДОВАНИЕ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Расследование инцидента информационной безопасности проводится с целью выявления и наказания лиц, виновных в инциденте, а также с целью выявления недоработок в политиках информационной безопасности и их оперативного устранения.

5.2. Расследование инцидента проводится Администратором безопасности самостоятельно (в случае незначительного инцидента) либо ГРИИБ (в случае значительного инцидента). В случаях, когда виновником инцидента является внешний нарушитель, к расследованию инцидента могут привлекаться сотрудники правоохранительных органов в установленном порядке.

5.3. Расследование инцидента проводится в следующем порядке:

- проводится сбор информации об инциденте из всех возможных источников, проводится анализ собранной информации, формируется доказательная база;
- анализируются каналы атаки, уязвимости и другие факторы, которые сделали возможным появление инцидента информационной безопасности;
- анализируются сценарии действий нарушителя, в случае антропогенной природы инцидента;
- составляется список подозреваемых в инциденте лиц, в случае антропогенной природы инцидента;
- выявляются лица, виновные в инциденте информационной безопасности, в случае антропогенной природы инцидента;
- определяется степень ущерба, нанесенная информационной системе, организации, субъектам персональных данных в результате инцидента информационной безопасности;
- составляется отчет о расследовании.

5.4. В случаях, если инцидент произошел по вине сотрудников ООО «БМЗ», руководство ООО «БМЗ» принимает решение о мерах, которые будут применены к виновному лицу.

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

5.5. В случаях, если инцидент произошел по вине контрагента или сотрудника сторонней организации, осуществляющей какие-либо работы в ООО «БМЗ», виновный в инциденте несет ответственность в соответствии с положениями договора между ООО «БМЗ» и контрагентом/сторонней организацией.

5.6. В случаях, если инцидент произошел по вине внешнего нарушителя, виновный несет ответственность в соответствии с уголовным и административным кодексами Российской Федерации.

5.7. После выявления и наказания виновных в инциденте, Администратором безопасности после согласования с руководством ООО «БМЗ» могут быть проведены занятия с сотрудниками ООО «БМЗ» по разбору произошедшего инцидента с целью предотвращения повторения инцидента в будущем.

5.8. Из каждого инцидента информационной безопасности извлекаются уроки, делаются выводы о необходимости изменения и улучшения организационных и технических частей системы защиты информации в ООО «БМЗ». Изменения в системе защиты информации, призванные предотвратить появление выявленного и расследованного инцидента информационной безопасности, должны быть осуществлены в кратчайшие сроки.

6. КЛАССИФИКАЦИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Инциденты ИБ по происхождению делятся на преднамеренные и случайные. Случайные инциденты могут быть вызваны антропогенными факторами (ошибка сотрудника, техническая неграмотность), социальными явлениями, природными явлениями, техногенными факторами (аварии, катастрофы).

6.2. Инциденты ИБ также можно разделить на инциденты, вызванные техническими средствами, и инциденты, вызванные нетехническими средствами.

6.3. В целом все инциденты безопасности можно разделить на следующие категории.

6.4. Одним из широко распространенных видов инцидентов ИБ является инцидент типа «Отказ в обслуживании». Результатом такого инцидента является неспособность систем, сервисов или сетей продолжать функционирование с прежней производительностью. Часто это сопровождается полным отказом в доступе авторизованным пользователям. Инциденты типа «отказ в обслуживании» могут быть вызваны как техническими, так и нетехническими средствами. Инциденты типа «отказ в обслуживании», вызываемые техническими средствами можно категорировать на инциденты, направленные на уничтожение ресурсов, и на инциденты, направленные на истощение ресурсов. Типовыми примерами таких преднамеренных технических инцидентов ИБ являются:

- зондирование сетевых широковещательных адресов с целью полного заполнения полосы пропускания сети трафиком ответных сообщений;

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

- передача данных в непредусмотренном формате в систему, сервис или сеть в попытке разрушить или нарушить их нормальную работу;
- одновременное открытие нескольких сеансов с конкретной системой, сервисом или сетью в попытке исчерпать их ресурсы.

Инциденты ИБ типа «Отказ в обслуживании», создаваемые нетехническими средствами и приводящие к утрате информации, сервиса и (или) устройств обработки информации, могут вызываться, например, следующими факторами:

- нарушения систем физической защиты, приводящие к хищениям, преднамеренному нанесению ущерба или разрушению оборудования;
- случайное нанесение ущерба техническим средствам и или месту их расположения от огня или воды;
- экстремальные условия окружающей среды, например высокая температура воздуха, вызванная выходом из строя системы кондиционирования воздуха;
- неправильной функционирование или перегрузка системы;
- неконтролируемые изменения в системе;
- неправильное функционирование программного и аппаратного обеспечения.

6.5. Инциденты ИБ типа «Сбор информации» подразумевают действия, связанные с определением потенциальных целей атаки и получением представления о сервисах, работающих на идентифицированных целях атаки. Подобные инциденты ИБ предполагают проведение разведки с целью определения:

- наличия цели, получения представления об окружающей ее сетевой топологии;
- потенциальных уязвимостей цели или непосредственно окружающей ее сетевой среды, которые можно использовать для атаки.

Типичными примерами атак, направленных на сбор информации техническими средствами, являются:

- сбрасывание записей DNS;
- отправка тестовых запросов по случайным сетевым адресам с целью найти работающие системы;
- зондирование системы с целью идентификации операционной системы хоста;
- сканирование доступных сетевых портов на протокол передачи файлов системе с целью идентификации соответствующих сервисов и версий программного обеспечения этих сервисов;
- сканирование одного или нескольких сервисов с известными уязвимостями по диапазону сетевых адресов.

ООО «БМЗ» | ИНН 5300000459 | КПП 530001001 | ОГРН 1215300004479
Юр. адрес: 174406, РФ, Новгородская обл., г. Боровичи, ул. Коммунарная, д. 25а/26
Производство Новгородская обл., г. Боровичи, ул. Окуловская, д. 12
8 (800) 700-11-33 | rus-man.com | info@rus-man.com

Инциденты, направленные на сбор информации, создаваемые нетехническими средствами, приводят к:

- прямому или косвенному раскрытию или модификации информации;
- хищению интеллектуальной собственности;
- нарушению учетности, например, при регистрации учетных записей;
- неправильному использованию информационных систем (например, с нарушением закона или политики организации).

Инциденты могут вызываться, например, следующими факторами:

- нарушениями физической защиты, приводящими к несанкционированному доступу к информации и хищению устройств хранения данных, содержащих значимые данные, например ключи шифрования;
- неудачно и (или) неправильно сконфигурированными операционными системами по причине неконтролируемых изменений в системе или неправильным функционированием программного или аппаратного обеспечения, приводящим к тому, что персонал организации или посторонний персонал получает доступ к информации, не имея на это разрешения.

6.6. Несанкционированный доступ как тип инцидента включает в себя инциденты, не вошедшие в первые два типа. Главным образом этот тип инцидентов состоит из несанкционированных попыток доступа в систему или неправильного использования системы, сервиса или сети. Некоторые примеры несанкционированного доступа с помощью технических средств включают в себя:

- попытки извлечь файлы с паролями;
- атаки переполнения буфера с целью получения привилегированного доступа к сети;
- использование уязвимостей протокола для перехвата соединения или ложного направления легитимных сетевых соединений;
- попытки расширить привилегии доступа к ресурсам или информации по сравнению с легитимно имеющимися у пользователя.

6.7. Более подробное описание угроз безопасности, а, следовательно, и возможности для возникновения инцидентов ИБ приведено в документе «Модель угроз безопасности информации.