УТВЕРЖДЕНО
Приказом генерального директора
ООО МКК «Равенство»
От «01» июля 2021г. № 4

ПОЛОЖЕНИЕ
ОБ ОБЕСПЕЧЕНИИ ЗАЩИТЫ
СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА
ООО МКК «Равенство»

Город Сарапул
2021 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обеспечении защиты сведений конфиденциального характера (далее – Положение) разработано в целях организации режима защиты информации, содержащей сведения конфиденциального характера, в том числе получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в автоматизированных системах, в отношении которой ООО МКК «***Равенство***» (далее – Организация) принимает меры по защите от несанкционированного доступа третьих лиц, не имеющих право доступа к такой информации (далее – Конфиденциальная информация).

1.2. Положение определяет систему защиты Конфиденциальной информации, в том числе вводит категорирование Конфиденциальной информации, регламентирует меры ее защиты, определяет обязанности работников и должностных лиц Организации по обеспечению ее защиты, а также ответственность за нарушение режима ее защиты с целью предотвращения нанесения возможного ущерба интересам и деловой репутации Организации, вызванного умышленными или неосторожными действиями работников Организации, других юридических и физических лиц вследствие разглашения (передачи, утраты) или незаконного присвоения такой информации, а также в целях противодействия осуществлению незаконных финансовых операций при осуществлении деятельности в сфере финансовых рынков.

1.3. Положение является внутренним документом, обязательным для выполнения всеми работниками Организации. Объем, в котором требования настоящего Положения распространяются на каждого работника Организации, зависит от должности работника и обусловлен его должностными обязанностями.

1.4. Защита Конфиденциальной информации не может быть использована работниками Организации для сокрытия фактов бесхозяйственности, недобросовестной конкуренции и других негативных явлений в деятельности Организации.

1.5. Настоящее Положение вступает в силу с момента его утверждения приказом руководителя Организации и действует без ограничения срока, до утверждения Положения в новой редакции.

2. ТЕРМИНЫ И СОКРАЩЕНИЯ

В настоящем Положении используются следующие термины и сокращения.

2.1. **Актуальные угрозы безопасности** - это совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к Конфиденциальной информации в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение Конфиденциальной информации, а также иные неправомерные действия.

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

2.3. **Информация, составляющая коммерческую тайну** – сведения любого характера (технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в сфере деятельности Организации, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

2.4. **Конфиденциальная информация** – информация, содержащая сведения конфиденциального характера, в том числе получаемая, подготавливаемая, обрабатываемая, передаваемая и хранимая в автоматизированных системах, в отношении которой Организация принимает меры по защите от несанкционированного доступа третьих лиц, не имеющих право доступа к такой информации.

2.5. **Криптографические ключи** – ключевая информация СКЗИ, используемая Организацией и ее клиентами при осуществлении финансовых операций.

2.6. **Несанкционированный доступ** – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим техническим характеристикам и функциональному назначению.

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

2.8. **Персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образования, профессия, доходы, другая информации.

2.9. **Реестр определения прав доступа к Конфиденциальной информации (далее – Реестр прав доступа)** – внутренний документ Организации, закрепляющий перечень должностей и категории Конфиденциальной информации, ресурсы информационной системы, криптографические ключи, к которым работники Организации имеют доступ.

2.10. **Режим конфиденциальности** – правовые, организационные, технические и иные меры по защите конфиденциальной информации, принимаемые ее обладателем на основании закона.

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

2.12. **СКЗИ** – ключевая информация средств криптографической защиты информации.

2.13. **Электронные сообщения** – информация, содержащаяся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками Организации и (или) клиентами Организации.

3. НОРМАТИВНОЕ РЕГУЛИРОВАНИЕ

3.1. Настоящее Положение разработано на основании следующих нормативных правовых и нормативных актов:

– Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ № 152);

– Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ № 149);

– Федеральный закон Российской Федерации от 29 июля 2004 г. №98-ФЗ «О коммерческой тайне» (далее – ФЗ № 98);

– Постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Положение Правительства РФ № 1119);

– Положения Банка России от 17 апреля 2019 г. № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при

осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» (далее – Положение Банка России № 684);

– Указания Банка России от 10 декабря 2015 г. № 3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных» (далее – Указание Банка России № 3889);

– Приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Приказ ФСТЭК № 21).

4. ОРГАНИЗАЦИЯ РАБОТЫ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

4.1. Безопасность Конфиденциальной информации, в том числе персональных данных, при ее использовании и обработке в Организации обеспечивается с помощью системы защиты Конфиденциальной информации, разработанной самой Организацией.

4.2. Система защиты Конфиденциальной информации реализуется путем проведения нескольких взаимосвязанных процессов. К ним относятся:

1) категорирование информации с целью определения информации, на которую распространяется режим конфиденциальности;
2) определение актуальных угроз безопасности Конфиденциальной информации, в том числе персональных данных;

   Организация определяет актуальные угрозы безопасности Конфиденциальной информации, в том числе персональных данных.

   Порядок определения актуальных угроз безопасности Конфиденциальной информации, в том числе персональных данных, и ответственный за проведение процедуры определения актуальных угроз безопасности Конфиденциальной информации, в том числе персональных данных, определяется приказом руководителя Организации.

   Результатом проведения процедуры определения актуальных угроз безопасности Конфиденциальной информации, в том числе персональных данных, является составление акта определения актуальных угроз безопасности Конфиденциальной информации.
3) определение необходимых правовых, организационных и технических мер по обеспечению безопасности Конфиденциальной информации, в том числе информации, содержащей персональные данные при их обработке в информационных системах персональных данных, исполнение которых обеспечивает необходимый уровень защищенности;

   Необходимый уровень защищенности Конфиденциальной информации, в том числе информации, содержащей персональные данные при их обработке в информационных системах персональных данных, определяется Организацией при выявлении актуальных угроз безопасности и фиксируется в акте определения актуальных угроз безопасности Конфиденциальной информации.
4) надлежащее применение определенных правовых, организационных и технических мер по обеспечению безопасности Конфиденциальной информации, в том числе информации, содержащей персональные данные при их обработке в информационных системах персональных данных, а так же применение прошедших в установленном

порядке процедуру оценки соответствия средств защиты Конфиденциальной информации;

5) проведение оценки эффективности принимаемых мер по обеспечению безопасности Конфиденциальной информации, в том числе информации, содержащей персональные данные, с установленной в настоящем Положении периодичностью;
6) обеспечение контроля надлежащей реализации мер по обеспечению безопасности Конфиденциальной информации, в том числе информации, содержащей персональные данные.

4.3. В целях обеспечения функционирования системы защиты Конфиденциальной информации руководитель Организации выполняет следующие функции:

– организация разработки проектов и утверждение внутренних документов Организации по вопросам обеспечения режима конфиденциальности, определения порядка обращения с Конфиденциальной информацией с привлечением иных работников Организации;

– организация взаимодействия с органами государственной власти, правоохранительными и надзорными органами по вопросам обеспечения и соблюдения режима конфиденциальности;

– утверждение Реестра прав доступа, в том числе при внесении изменений и дополнений;

– рассмотрение вопроса о передаче Конфиденциальной информации третьим лицам;

– рассмотрение предложений о снятии ограничений на доступ к Конфиденциальной информации, а также о возможности опубликования такой информации на общедоступных ресурсах (раскрытия);

– определение требований к техническому оснащению помещений, в которых осуществляется работа с Конфиденциальной информацией;

– осуществление контроля за обеспечением режима безопасности помещений;

– принятие решений о необходимости проведения обучений для работников Организации;

– проведение плановых и внезапных проверок на предмет соблюдения режима конфиденциальности в Организации работниками Организации;

– принятие решений о необходимости отстранения от работы с Конфиденциальной информацией работников Организации, нарушающих режим конфиденциальности в Организации;

– рассмотрение иных вопросов обеспечения и соблюдения режима конфиденциальности.

5. КАТЕГОРИРОВАНИЕ ИНФОРМАЦИИ ПО СТЕПЕНИ КОНФИДЕНЦИАЛЬНОСТИ

5.1. Данным Положением в Организации вводятся следующие категории информации:

– Конфиденциальная информация;

– Общедоступная информация.

5.2. Конфиденциальная информация – это информация, в отношении которой Организацией применяются меры по защите, в соответствии с требованиями Федеральных законов, подзаконных нормативных актов и иных нормативных актов.

5.3. К Конфиденциальной информации относится:

– информация, составляющая коммерческую тайну Организации;

– информация, содержащаяся в Электронных сообщениях;

– информация, необходимая Организации для авторизации своих клиентов в целях осуществления финансовых операций;

– информация об осуществленных Организацией и ее клиентами финансовых операций;

– Криптографические ключи;
– информация, содержащая персональные данные работников, клиентов, контрагентов Организации. К такой информации относится, в том числе информация, перечисленная в подпунктах 1-5 настоящего пункта в случае, если указанная информация содержит персональные данные работников, клиентов, контрагентов Организации.

5.3.1. Сведения, составляющие Конфиденциальную информацию, определяются Реестром прав доступа. Реестр прав доступа, является единым для всей Организации и утверждается приказом руководителя Организации. Изменения и дополнения к Реестру прав доступа вносятся в него приказом руководителя Организации.

5.3.2. Информация, составляющая коммерческую тайну Организации. Право на отнесение информации к информации, составляющей коммерческую тайну и на определение перечня и состава такой информации, принадлежит Организации, за исключением информации, содержащей сведения, перечисленные в ст. 5 ФЗ № 98.

5.3.3. Информация, содержащаяся в Электронных сообщениях.

К информации, содержащейся в Электронных сообщениях, относятся все документы в электронном виде, содержащие информацию об осуществлении финансовых операций, Организацией и (или) клиентом, в том числе при их взаимодействии.

5.3.4. Информация, необходимая Организации для авторизации своих клиентов в целях осуществления финансовых операций.

К информации, необходимой Организации для авторизации своих клиентов в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом, относятся вся информация, содержащая сведения об аутентификации/идентификации клиентов Организации.

5.3.5. Информация об осуществленных Организацией и ее клиентами финансовых операциях.

К информации об осуществленных Организацией и ее клиентами финансовых операциях относится вся информация, содержащая сведения об осуществляемых финансовых операциях Организацией или клиентами, в том числе передаваемая в установленном законом порядке третьим лицам на основании обязанностей Организации.

5.3.6. Криптографические ключи.

К Криптографическим ключам относятся все аппаратные устройства или программные обеспечения, используемые Организацией для шифрования Конфиденциальной информации.

5.3.7. Информация, содержащая персональные данные работников, клиентов и контрагентов Организации.

К информации, содержащей персональные данные работников, клиентов и контрагентов Организации относятся все документы, в том числе в электронной форме, содержащие персональные данные.

Режим обеспечения защиты информации, содержащей персональные данные работников, клиентов и контрагентов Организации, устанавливается Положением о защите персональных данных работников, клиентов и контрагентов Организации. Информация, содержащая персональные данные всегда относится к категории Конфиденциальной информации, за исключением случаев:

– обезличивания персональных данных;
– иных случаях установленных Федеральным законом «О персональных данных» и иными федеральными законами.

5.4. Общедоступная информация – это информации, в отношении которой Организацией не применяются меры по защите.

К данной категории относится любая другая информация, не отнесенная к Конфиденциальной информации, а также информация, определяемая законом как общедоступная.

6. ПРАВОВЫЕ МЕРЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

6.1. К правовым мерам защиты Конфиденциальной информации относится:

6.1.1. разработка локальных нормативных актов Организации, регламентирующих порядок организации системы защиты (далее – Регламентирующие документы). К ним относятся:

- Настоящее Положения;
- Положение о защите персональных данных работников, клиентов и контрагентов Организации;
- Положение по обеспечению безопасности помещений;
- Иных документов.

6.1.2. обязанность Организации осуществлять мониторинг действующего законодательства.

6.2. Регламентирующие документы разрабатываются самой Организацией или с привлечением третьих лиц и утверждаются руководителем Организации.

6.3. Регламентирующие документы должны пересматриваться на предмет их актуальности и необходимости внесения изменений не реже одного раза в год, а также:

- в случае изменения законодательства, регламентирующего порядок обращения организаций с Конфиденциальной информацией и устанавливающего требования к защите информации, в том числе законодательства о персональных данных;
- в случае установления фактов несанкционированного доступа к Конфиденциальной информации, грубого нарушения работниками Организации режима конфиденциальности, разглашения и утечки Конфиденциальной информации;
- на основании заключения, сформированного по результатам проведения очередной оценки достаточности принятых мер по защите Конфиденциальной информации.

6.4. Предложения по внесении изменений в документы, указанные в п. 6.1.1 настоящего Положения, могут вноситься лицом, ответственным за информационную безопасность, а также иными работниками Организации.

7. ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

К организационным мерам защиты Конфиденциальной информации относятся:

7.1. Определение правил доступа к Конфиденциальной информации.

7.1.1. К работе с Конфиденциальной информацией могут быть допущены работники Организации при одновременном выполнении следующих условий:

- должность работника указана в Реестре прав доступа;
- работник ознакомлен под подпись с Реестром прав доступа и настоящим Положением;
- работником Организации подписано Обязательство о неразглашении информации.

7.1.2. Приказом руководителя Организации с целью определения перечня лиц, доступ которых к Конфиденциальной информации необходим для выполнения ими своих должностных обязанностей, и определения необходимого объема Конфиденциальной информации, с которым вправе работать каждый из таких сотрудников, утверждается Реестр прав доступа.

1) При утверждении Реестра прав доступа Организация руководствуется правилом о том, что доступ к Конфиденциальной информации должен предоставляться только тем лицам, которым Конфиденциальная информация необходима для выполнения возложенных на них должностных обязанностей и только в том объеме (к той ее части), который необходим для выполнения определенных функций.

2) Реестр прав доступа Организации содержит следующую информацию:

- должности работников Организации, допущенных к работе с Конфиденциальной информацией;
- категории Конфиденциальной информации, к которым работники имеют доступ;
- Ресурсы информационной системы, к которым работники имеют доступ;
- Криптографические ключи, к которым работники имеют доступ.

3) Реестр прав доступа подлежит обязательному пересмотру не реже одного раза в год, а также в случае:

- изменения штатного расписания Организации;
- изменения функционала определенной должности;
- изменения перечня Ресурсов информационной системы;
- приобретения или уничтожения Криптографических ключей.

4) Правом предоставления, ограничения, прекращения доступа ко всей Конфиденциальной информации, создаваемой, хранимой и обрабатываемой в Организации, включая информацию, полученную от третьих лиц, обладает руководитель Организации.

7.1.3. До начала работы с Конфиденциальной информацией работник должен подписать обязательство о неразглашении Конфиденциальной информации.

Обязательство о неразглашении Конфиденциальной информации, подписанное работником Организации, приобщается к личному делу работника.

7.1.4. Определение обязанностей для работников Организации при работе с Конфиденциальной информацией.

Работник Организации, допущенный к работе с Конфиденциальной информацией, обязан:

- знать и выполнять требования настоящего Положения, иных внутренних документов по защите информации;
- соблюдать ограничения, установленные Реестром прав доступа: знакомиться только с теми сведениями и использовать только те Ресурсы информационной системы, которые определены в соответствии с Реестром прав доступа;
- соблюдать порядок работы и меры по защите ставших ему известными сведений конфиденциального характера;
- соблюдать правила работы с носителями Конфиденциальной информации, порядок их учета и хранения, обеспечивать в процессе работы сохранность сведений, содержащихся в них от посторонних лиц;
- незамедлительно в письменной форме, информировать руководителя Организации о попытках несанкционированного доступа к информационным ресурсам и сведениям, содержащим Конфиденциальную информацию, о попытках подкупа, угроз, шантажа другими лицами с целью получения доступа к Конфиденциальной информации;
- давать письменные объяснения о допущенных личных нарушениях установленного порядка работы, учета и хранения документов, содержащих Конфиденциальную информацию, и машинных съемных носителей информации, а также о фактах их утраты, передачи другим лицам.

7.1.5. Определение ограничений для работников Организации при работе с Конфиденциальной информацией.

Работнику, допущенному к работе с Конфиденциальной информацией, запрещается:

- передавать сведения конфиденциального характера и документы (в устной форме, по телефону, на бумажных и машинных носителях, в электронной виде и т.д.) другим лицам;
- использовать Конфиденциальную информацию Организации в открытой переписке, статьях и выступлениях, а также в личных интересах;
- передавать по незащищенным техническим каналам связи, в том числе сообщать (обсуждать) по телефону сведения конфиденциального характера;
- снимать копии с документов, содержащих Конфиденциальную информацию, или производить выписки из них;
- копировать документы, содержащие Конфиденциальную информацию Организации, и хранить ее на машинных съемных носителях информации, а также использовать различные технические средства, способные накапливать и хранить информацию в электронном виде (фото, видео и звукозаписывающую аппаратуру, сотовые телефоны и т.п.), за исключением случаев, описанных в настоящем Положении;
- выполнять работы материальными и машинными носителями, содержащими Конфиденциальную информацию, вне служебных помещений (помещений, где размещены подразделения Организации);
- выносить из служебных помещений документы и машинные носители с Конфиденциальной информацией.

7.1.6. Установление ответственности за разглашение Конфиденциальной информации.

Работники Организации несут персональную ответственность за нарушение режима конфиденциальности, установленного в Организации.

Лица, виновные в нарушении режима конфиденциальности, несут предусмотренную законодательством Российской Федерации ответственность.

7.2. Назначение лица, ответственного за информационную безопасность.

Приказом руководителя Организации назначается лицо, ответственное за информационную безопасность. В число его обязанностей входят:

- организация процесса реализации норм, установленных настоящим Положением, в том числе обеспечение работы системы защиты Конфиденциальной информации;
- обеспечение применения в Организации определенных мер защиты Конфиденциальной информации;
- контроль за соблюдением работниками Организации требований настоящего Положения;
- Проведение обучений для работников Организации в целях ознакомления с требованиями настоящего Положения;
- сбор и анализ статистических данных об Актуальных угрозах безопасности, характерных для Организации;
- внесение предложений руководителю Организации о необходимости проведения оценки достаточности принятых мер по защите Конфиденциально информации, предложений по внесению изменений во внутренние документы Организации, регламентирующие деятельность Организации по защите Конфиденциально информации, предложений по

иным вопросам, связанным с деятельностью Организации по защите Конфиденциально информации.

7.3. Определение порядка передачи Конфиденциальной информации.

7.3.1. Конфиденциальная информация может быть передана третьим лицам по письменному запросу третьего лица и только с письменного разрешения руководителя Организации, при условии соблюдения требований действующего законодательства:

- по требованию органов государственной власти и местного самоуправления, государственных, надзорных и контролирующих органов, а также участников Организации в соответствии с действующим законодательством;
- работникам Организации в соответствии с учредительным документом Организации;
- другим физическим и юридическим лицам на основании гражданско-правовых договоров, заключенных между ними и Организацией, при условии наличия в этих договорах обязательств по соблюдению режима конфиденциальности в отношении информации, ответственности за разглашение этой информации или заключения с ними отдельного договора о конфиденциальности.

7.3.2. Необходимость (возможность) передачи Конфиденциальной информации для открытого опубликования (раскрытия), ее объем, форму, и время опубликования (раскрытия) определяет руководитель Организации. Под открытым опубликованием (раскрытием) Конфиденциальной информации понимается ее публикация в открытой печати, компьютерных информационных сетях общего пользования, передача по радио и телевидению, передача ее в любой форме организациям или отдельным лицам, с которыми не заключен договор о конфиденциальности.

7.3.3. Порядок передачи Конфиденциальной информации внутри Организации и третьим лицам на бумажных и съемных машинных носителях информации определяется настоящим Положением.

Передача Конфиденциальной информации, представленной в электронном виде (документы, файлы, базы данных, архивы) через сети передачи данных должна осуществляться исключительно в зашифрованном виде, при условии, что только обменивающимся сторонам доступны секретные ключи шифрования (пароли).

7.4. Обеспечение сохранности носителей информации.

7.4.1. Режим сохранности материальных носителей информации.

1) Доступ к материальным носителям Конфиденциальной информации имеют только те работники Организации, которым такая информация необходима для выполнения должностных обязанностей.

2) Доступ к материальным носителям Конфиденциальной информации посторонним лицам запрещен.

3) Материальные носители, содержащие Конфиденциальную информацию, должны храниться в специальных сейфах или запирающихся металлических шкафах.

7.4.2. Режим сохранности машинных носителей информации.

1) Учет машинных носителей информации осуществляется лицом, ответственным за информационную безопасность, путем ведения журнала учета машинных носителей информации. В журнале учета машинных носителей информации каждый машинный носитель информации Организации закрепляется за ответственным работником, который не вправе передавать закрепленный за ним машинный носитель информации третьим лицам.

2) Запрещается копирование файлов с Конфиденциальной информацией и хранение их на жестких дисках рабочих станций (компьютеров, ноутбуков), съемных машинных носителях

информации, других устройствах, способных накапливать и хранить информацию в электронном виде, за исключением случаев, описанных в настоящем Положении.

3) Организация приобретает съемные машинные носители информации, способные накапливать и хранить информацию, для использования работниками Организации в рабочих целях. Такие машинные носители должны проверяться на наличие вирусов и вредоносных программ на регулярной основе.

7.5. Определение порядка подготовки и проведения совещаний, встреч, переговоров, аудио и видеоконференций, связанных с обсуждением сведений, содержащих Конфиденциальную информацию.

7.5.1. Проведение совещаний, встреч, переговоров, аудио и видеоконференций, телефонных переговоров связанных с обсуждением сведений конфиденциального характера без принятия специальных мер, изложенных ниже, не допускается:

1) Совещания, встречи, переговоры, аудио и видеоконференции, связанные с обсуждением сведений конфиденциального характера должны проводиться в специально выделенных помещениях для проведения совещаний, встреч, переговоров, аудио и видеоконференций, связанных с обсуждением сведений конфиденциального характера.

2) Доступ в такие помещения должен быть ограничен кругом лиц, участвующих (приглашенных) в совещании.

3) Запрещается проведение аудио- и видеоконференций, связанных с обсуждением сведений конфиденциального характера без принятия специальных мер защиты информации, передаваемой по незащищенным каналам связи.

4) Запрещается использование фото-, видео-, аудиозаписи, мобильных телефонов, диктофонов и других технических средств регистрации информации, в том числе, встроенных в портативные и карманные компьютеры, мобильные телефоны, без разрешения должностного лица Организации, ответственного за проведение мероприятия.

7.6. Установление режима использования Криптографических ключей.

7.6.1. Организация осуществляет учет Криптографических ключей путем закрепления права их использования за определенным должностным лицом в Реестре прав доступа. При этом каждый Криптографический ключ используется только руководителем Организации или работником, должность которого определена в Реестре прав доступа.

7.6.2. Передача Криптографических ключей, в случае если Криптографический ключ размещен на материальном носителе, не допустима.

7.6.3. Криптографические ключи должны использоваться Организацией в соответствии с технической документацией.

7.7. Установление режима обеспечения безопасности помещений.

7.7.1. В целях исключения возможности неконтролируемого проникновения или пребывания в помещениях, в которых обрабатывается и(или) хранится Конфиденциальная информация, посторонних лиц Организация устанавливает режим обеспечения безопасности этих помещений.

7.7.2. Требования к помещениям в которых обрабатывается и(или) хранится Конфиденциальная информация, а также правила доступа к таким помещениям устанавливаются в положении по обеспечению безопасности помещений, которое утверждается руководителем Организации.

7.8. Обнаружение фактов несанкционированного доступа к Конфиденциальной информации, а также фактов нарушения работниками режима конфиденциальности и принятие мер.

7.8.1. Организация принимает меры по обнаружению фактов несанкционированного доступа путем:

- установления обязанности работников сообщать о фактах, свидетельствующих о несанкционированном доступе к Конфиденциальной информации, в том числе о фактах несанкционированного проникновения в помещения, в которых обрабатывается и(или) хранится Конфиденциальная информация;
- применения технических средств обнаружения фактов несанкционированного доступа в информационную систему.

7.8.2. Каждый факт несанкционированного доступа фиксируется лицом, ответственным за информационную безопасность, в определенном им порядке.

7.8.3. По всем фактам нарушений работниками режима конфиденциальности должны быть проведены расследования, в ходе которых определен круг лиц, виновных в этих нарушениях и причастных к ним, а также причины и условия, способствовавшие совершению данных нарушений. К проведению расследования привлекается лицо, ответственное за информационную безопасность.

7.8.4. По каждому факту несанкционированного доступа к Конфиденциальной информации, а также факту нарушения работниками режима конфиденциальности проводится анализ причин и условий, совершению указанных фактов, по результатам которого составляется заключение, содержащее дополнительные меры по защите Конфиденциальной информации, а также план по реализации данных мер, включающий сроки их реализации и ответственных лиц.

8. ТЕХНИЧЕСКИЕ МЕРЫ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

К техническим мерам защиты Конфиденциальной информации относятся:

8.1. Приобретение и установка антивирусного программного обеспечения.

Обязательным условием для приобретения антивирусного программного обеспечения является наличие лицензии. Антивирусное программное обеспечение должно регулярно обновляться в соответствии с последней версией. Антивирусное программное обеспечение устанавливается на все персональные компьютеры информационной системы Организации.

8.2. Создание учетных записей для работников Организации.

8.3. Каждому пользователю информационной системы Организации, работающему с Конфиденциальной информацией, присваиваются личная учетная запись, для входа в которую устанавливается пароль. Пароль для входа в учетную запись не может совпадать с паролем для входа в учетные записи иных работников Организации. Пароль для входа в учетную запись не может передаваться третьим лицам, за исключением случаев, установленных настоящим Положением.

8.4. Установление режима защиты сетевого взаимодействия.

8.4.1. Обмен данными между элементами информационной системы Организации и другими компьютерами (рабочими станциями, серверами) должен быть организован через защищенные соединения, организованные с использованием протоколов IPSec с проверкой подлинности и шифрованием IP-пакетов.

8.5. Осуществление Резервного копирования Конфиденциальной информации.

8.6. Ограничение доступа к Информационно-коммуникационной сети Интернет.

Пользователям информационной системы Организации (учетным записям пользователей), работающим с Конфиденциальной информацией, может быть ограничен доступ к сети Интернет и средствам электронной почты.

8.7. Применение технических средств, обеспечивающих восстановление модифицированной или уничтоженной вследствие несанкционированного доступа Конфиденциальной информации, в том числе информации, содержащей персональные данные.

9. ПРОВЕДЕНИЕ ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРИНЯТЫХ МЕР ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

9.1. Оценка эффективности принятых мер по защите Конфиденциальной информации может проводиться Организацией самостоятельно или с привлечением сторонней организации.
9.2. Оценка эффективности принятых мер по защите Конфиденциальной информации проводится по результатам внутренней проверки, проводимой лицом, ответственным за информационную безопасность.
9.3. Приказом руководителя утверждаются периодичность проведения проверок (но не реже одного раза в год), сроки проведения плановых проверок, а также их содержание.
9.4. Помимо плановых проверок, предусмотренных в пункте 9.3, могут проводиться внеплановые проверки в случае наличия подозрений в возможном нарушении системы защиты Конфиденциальной информации.
9.5. По результатам проведения проверок составляется письменный отчет, который должен содержать:

- сведения обо всех фактах несанкционированного доступа к Конфиденциальной информации, нарушения работниками режима конфиденциальности;
- предложения по внесению изменений в систему защиты Конфиденциальной информации и представляет руководителю Организации заключение о проведении оценки достаточности принятых мер по защите Конфиденциальной информации.

9.6. Руководитель Организации на основании подготовленного лицом, ответственным за информационную безопасность, отчета принимает одно из следующих решений:

- о необходимости принятия дополнительных мер по защите Конфиденциальной информации;
- об отсутствии необходимости принятия дополнительных мер по защите Конфиденциальной информации.

9.7. В случае принятия решения о недостаточности принятых мер по защите Конфиденциальной информации руководитель Организации принимает решение о необходимости применения дополнительных мер по изменению системы защиты Конфиденциальной информации в целях приведения ее к достаточному уровню.

10. ОСУЩЕСТВЛЕНИЕ КОНТРОЛЯ

10.1. Контроль за соблюдением работниками Организации требований, предъявляемых к ним и установленных настоящим Положением, осуществляется лицом, ответственным за информационную безопасность.
10.2. Контроль за реализацией настоящего Положения, внедрения требований настоящего Положения в систему защиты Конфиденциальной информации, обеспечение системного подхода при реализации мер по защите Конфиденциальной информации осуществляется руководителем Организации.

ЛИСТ ОЗНАКОМЛЕНИЯ

№ п/п	Дата:	ФИО:	Должность:	Подпись: