Приложение к приказу №3 от «15»03 2017г. ООО «КАДРОВЫЙ ОПЕРАТОР ВАКАНСИЯ.

Положение
о порядке организации и проведения работ
по защите конфиденциальной информации

1. Общие положения

1.1. Настоящее Положение определяет порядок организации и проведения работ по защите конфиденциальной информации в Общество с ограниченной ответственностью «КАДРОВЫЙ ОПЕРАТОР ВАКАНСИЯ 22»,.

1.2. Мероприятия по защите конфиденциальной информации, проводимые в ООО «КАДРОВЫЙ ОПЕРАТОР ВАКАНСИЯ 22», являются составной частью управленческой и иной служебной деятельности и осуществляются во взаимосвязи с мерами по обеспечению установленной конфиденциальности проводимых работ.

1.3. Режим защиты конфиденциальной информации устанавливается в соответствии с законодательством.

Конфиденциальная информация должна обрабатываться (передаваться) с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств технической защиты конфиденциальной информации, сертифицируемых в установленном порядке. Обязательной сертификации подлежат средства, в том числе иностранного производства, предназначенные для технической защиты конфиденциальной информации.

1.4. Уровень технической защиты конфиденциальной информации, а также перечень необходимых мер защиты определяется дифференцировано по результатам обследования объекта информатизации, с учетом соотношения затрат на организацию технической защиты конфиденциальной информации и величины ущерба, который может быть нанесен собственнику конфиденциальной информации при ее разглашении, утрате, уничтожении и искажении. Для сведений, составляющих служебную тайну не ниже требований, установленных данным документом и государственными стандартами Российской Федерации.

Системы и средства информатизации и связи, предназначенные для обработки (передачи) конфиденциальной информации должны быть аттестованы в реальных условиях эксплуатации на предмет соответствия принимаемых мер и средств защиты требуемому уровню безопасности информации.

Проведение любых мероприятий и работ с конфиденциальной информацией, без принятия необходимых мер технической защиты информации не допускается.

1.5. Объектами защиты в ООО «КАДРОВЫЙ ОПЕРАТОР ВАКАНСИЯ 22», являются:

- средства и системы информатизации и связи (средства вычислительной техники, средства, системы связи и передачи информации, средства звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления и тиражирования документов), используемые для обработки, хранения и передачи информации, содержащей конфиденциальную информацию - далее основные технические средства и системы (ОТСС);
- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается конфиденциальной информация - далее вспомогательные технические средства и системы (ВТСС);
- помещения (служебные кабинеты), специально предназначенные для проведения конфиденциальных мероприятий – защищаемые помещения (ЗП).

1.6. Ответственность за выполнение требований настоящего Положения возлагается на ответственного сотрудника, а также на специалистов допущенных к обработке, передаче и хранению в технических средствах информации, содержащей конфиденциальную информацию.

1.7. Непосредственное руководство работами по защите конфиденциальной информации осуществляет ответственный сотрудник – директор ООО «КАДРОВЫЙ ОПЕРАТОР ВАКАНСИЯ 22»,.

2. Охраняемые сведения

2.1. В ООО «КАДРОВЫЙ ОПЕРАТОР ВАКАНСИЯ 22» разрабатывается Перечень сведений конфиденциального характера. Сведения, составляющие конфиденциальную информацию, определяются Перечнем сведений конфиденциального характера в соответствии с Указом Президента РФ от 6 марта 1997 года № 188.

3. Технические каналы утечки конфиденциальной информации, несанкционированного доступа и специальных воздействий на нее.

3.1. Доступ к конфиденциальной информации, нарушение ее целостности и доступности возможно реализовать за счет:

– несанкционированного доступа к конфиденциальной информации при ее обработке в информационных системах и ресурсах;

– утечки конфиденциальной информации по техническим каналам.

3.2. Детальное описание возможных технических каналов утечки информации, несанкционированного доступа к информации и специальных воздействий на нее содержится в Модели угроз безопасности информации ООО «КАДРОВЫЙ ОПЕРАТОР ВАКАНСИЯ 22».

4.Оценка возможностей технических разведок и других источников угроз безопасности конфиденциальной информации

4.1. Для добывания конфиденциальных сведений могут использоваться:

портативная возимая (носимая) аппаратура радио, акустической, визуально-оптической и телевизионной разведки, а также разведки побочных электромагнитных излучений и наводок (ПЭМИН);

автономная автоматическая аппаратура акустической и телевизионной разведки, а также разведки ПЭМИН;

компьютерная разведка, использующая различные способы и средства несанкционированного доступа к информации и специальных воздействий на нее.

Угроза компьютерной разведки объектам защиты возможна в случае подключения АС, обрабатывающим информацию ограниченного доступа к внешним, в первую очередь - глобальным сетям.

4.2. Несанкционированный доступ к информации и специальные воздействия на нее могут осуществляться при ее обработке на отдельных автоматизированных рабочих местах, в локальных вычислительных сетях, в распределенных телекоммуникационных системах.

4.3. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, вследствие:

– непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций защищаемых помещений и их инженерно-технических систем;

– случайного прослушивания телефонных разговоров при проведении профилактических работ в сетях телефонной связи;

– некомпетентных или ошибочных действий пользователей и администраторов АС при работе вычислительных сетей;

– просмотра информации с экранов дисплеев и других средств ее отображения.