

УТВЕРЖДЕНО
Советом директоров ОАО «НПО СЭМ»
Протокол № 6 от 23 апреля 2012 года
Председатель Совета директоров
ОАО «НПО СЭМ»

_____ (Лановенко С.Б.)

П О Л О Ж Е Н И Е
о конфиденциальной информации (коммерческая тайна),
инсайдерской информации
и персональных данных сотрудников
ОАО «НПО СЭМ»

1. Общие положения.

1.1. Настоящее Положение разработано в соответствии с Гражданским кодексом РФ, Федеральным законом «О коммерческой тайне», Федеральным законом «О персональных данных», Федеральным законом «Об акционерных обществах» и другими действующими нормативно-правовыми актами. Настоящее Положение устанавливает порядок использования и защиты конфиденциальной информации (коммерческая тайна), инсайдерской информации ОАО «НПО» (далее компания), а также персональных данных сотрудников компании.

1.2. Положение утверждается Советом директоров ОАО «НПО». Предложения о внесении изменений и дополнений в настоящее Положение вносятся в повестку дня заседания общего собрания акционеров. Любая иная информация, не внесенная в данное Положение, может быть отнесена к конфиденциальной по решению Совета директоров ОАО «НПО СЭМ».

1.3. Определения, употребляемые в настоящем Положении:

- *конфиденциальная информация (коммерческая тайна)* - любая информация о компании (производственная, техническая, организационная и др.), связанная с созданием и деятельностью компании, имеющая потенциальную коммерческую ценность в силу неизвестности ее третьим лицам и отсутствия свободного доступа к ней на законных основаниях, в отношении которой компания принимает меры к охране ее конфиденциальности, а также знания и опыт, обладание которыми дает определенную экономическую выгоду;
- *инсайдерская информация* – любая информация об эмиссионных ценных бумагах компании и сделках с ними, а также о компании и осуществляемой деятельности, не известной третьим лицам, раскрытие которой может оказать существенное влияние на рыночную цену ценных бумаг;
- *инсайдер* – лицо, которое имеет доступ к инсайдерской информации в силу участия в уставном капитале компании или его аффилированного лица, членства в органах управления компанией или его аффилированного лица, заключенного с эмитентом или его аффилированным лицом трудового договора или имеющее доступ к инсайдерской информации;
- *персональные данные* – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника, а также сведения о фактах, событиях и обстоятельствах жизни сотрудника, позволяющая идентифицировать его личность;
- *сотрудники* – все работники компании, включая руководителей подразделений (отделов) и генерального директора.

2. Конфиденциальная информация (коммерческая тайна).

2.1. К конфиденциальной информации компании относятся сведения:

- о руководителях и работниках компании;
- об участии компании в уставных капиталах (фондах) других организаций, о вложении средств компании в ценные бумаги;
- об организационной структуре компании;
- об акционерах компании (в т.ч. персональные данные);
- о проводимых собраниях акционеров компании, а также решениях, принятых на них;
- о рыночной стратегии компании;
- о структуре службы безопасности, охраны, пропускном режиме, системе сигнализации;
- о финансовом состоянии компании и финансовых операциях;
- о состоянии материально-технической базы компании;
- нормативы, используемые в составлении бухгалтерских отчетов;

- содержание регистров бухгалтерского учета и внутренней бухгалтерской отчетности;
- о порядке и состоянии организации защиты конфиденциальной информации (коммерческой тайны), охраны, пропускном режиме, системе сигнализации компании;
- о режиме хранения печатей, чистых бланков, договоров (контрактов) компании с контрагентами, а также о местонахождении оригиналов, ксерокопий и текстов этих договоров, доступе к ним, в том числе записей на магнитных носителях и в электронных (компьютерных) базах данных компании;
- касающиеся интересов личности акционеров (участников) и работников компании, которые они считают необходимым сохранять в качестве конфиденциальных;
- о документообороте компании.

2.2. К сведениям, составляющим коммерческую тайну компании, относятся:

- объекты интеллектуальной деятельности и научно-технические разработки (открытия, изобретения, рационализаторские предложения, полезные модели, конструкции, промышленные образцы, базы данных, секреты производства);
- нормативно-технологическая и конструкторская документация;
- состав поставщиков и потребителей продукции, товаров, услуг и сырья;
- номенклатура выпускаемой продукции (не перечисленной в прайс-листах);
- содержание конкретных предпринимательских договоров;
- себестоимость выпускаемой продукции, структура цены и условия конкретных сделок;
- сведения о предполагаемом спросе и предложении на продукцию, товары и услуги компании, о планах расширения или свертывания производства различных видов продукции, о применяемых компанией оригинальных методах изучения рынка и методах осуществления продаж, о результатах изучения рынка, содержащие оценки состояния и перспектив развития рыночной конъюнктуры, о рыночной стратегии компании и эффективности ее коммерческой деятельности;
- сведения о подготовке и результатах проведения переговоров с деловыми партнерами компании;
- служебные сведения, доступ к которым ограничен, тайна переписки, телефонных переговорах, почтовых, телеграфных и иных сообщений;
- любые специальные знания, включая практический опыт специалистов, имеющие коммерческую ценность и разглашение которых может повлечь за собой причинение ущерба компании.

2.3. К конфиденциальной информации (коммерческой тайне) не относится:

- общедоступная информация;
- информация, ставшая известной из публичных источников;
- информация, которая не может являться конфиденциальной в соответствии с законодательством Российской Федерации.

3. Режим обеспечения конфиденциальной информации (коммерческая тайна) (далее – конфиденциальная информация).

3.1. При приеме на работу, сотрудник компании подписывает обязательство о соблюдении режима конфиденциальной информации. Состав и перечень сведений, отнесенных к конфиденциальной информации, доводится до его сведения путем ознакомления с настоящим Положением.

3.2. Информация, составляющая конфиденциальную информацию, может быть разглашена сотрудниками компании с разрешения генерального директора компании только в тех случаях, когда это требуется для выполнения своих служебных обязанностей и только тем лицам, с которыми сотрудник компании уполномочен общаться в своем официальном качестве (во исполнение своих функциональных обязанностей).

3.3. Если сотрудник компании будет обязан по закону раскрыть конфиденциальную информацию компетентным органам государства, он должен незамедлительно уведомить об этом генерального директора компании.

3.4. Сотрудники компании обязаны работать только с теми сведениями и документами, содержащими конфиденциальную информацию, доступ к которым он получил в силу своих служебных обязанностей.

3.5. Запрещается помещать сведения, составляющие конфиденциальную информацию, в документы открытого характера. Такое нарушение порядка обращения со сведениями, составляющими конфиденциальную информацию, рассматривается как их разглашение и влечет ответственность в соответствии с установленным порядком.

3.6. Сотрудник компании обязан сообщать непосредственному руководителю обо всех фактах утраты, хищения, недостачи носителей конфиденциальной информации, а также удостоверений, пропусков, ключей от служебных помещений, сейфов (металлических шкафов) и о других фактах, которые могут привести к разглашению конфиденциальной информации, а также о причинах и условиях возможной утечки информации.

3.7. В случае попытки посторонних физических или юридических лиц получить информацию, составляющую конфиденциальную информацию, сотрудник компании обязан немедленно сообщить об этом своему непосредственному руководителю.

3.8. Сотрудники компании обязаны сохранять в тайне полученную ими в процессе выполнения служебных обязанностей конфиденциальную информацию в течение всего периода работы в компании, а при увольнении (в том числе как не прошедшие испытательный срок, либо в случае расторжения трудового договора) – не разглашать конфиденциальную информацию в течение трех лет с момента прекращения трудовых отношений с компанией.

4. Нарушение режима обеспечения конфиденциальной информации (коммерческая тайна) (далее – конфиденциальная информация).

4.1. Нарушением режима обеспечения конфиденциальной информации следует считать следующие действия сотрудника компании, совершенные им в случаях, когда законодательство или настоящее Положение прямо не обязывали его их совершить, либо при отсутствии письменного согласия на это генерального директора компании, либо при отсутствии обстоятельств, которые бы уполномочивали его к этому:

4.1.1. Доведение до сведения неуполномоченных лиц в устной, письменной, электронной или иной форме сведений, отнесенных к конфиденциальной информации. Указанный факт может наступить в результате умысла сотрудника, или по его неосторожности, включая халатное отношение к своим обязанностям. Эти действия могут быть связаны с нарушением требований действующего законодательства, трудового договора, настоящего Положения, иных обязательных для исполнения правил, направленных на предупреждение случаев разглашения конфиденциальной информации.

4.1.2. Использование сведений, составляющих конфиденциальную информацию в ходе публичных выступлений, интервью и т.п.

4.1.3. Сотрудники компании несут ответственность за разглашение и использование конфиденциальной информации в корыстных целях или в интересах третьих лиц.

5. Инсайдерская информация.

5.1. К инсайдерской информации относится информация, составляющая коммерческую тайну в соответствии с гражданским законодательством Российской Федерации, а также информация, подлежащая раскрытию в соответствии с законодательством Российской Федерации о рынке ценных бумаг, до момента ее раскрытия.

5.2. Сведения, содержащие оценку стоимости ценных бумаг и (или) оценку имущественного положения эмитента, произведенную на основе общедоступной информации, не относятся к инсайдерской информации.

6. Использование инсайдерской информации.

6.1. Инсайдеры, а также их аффилированные лица не вправе:

- совершать сделки с ценными бумагами, с использованием инсайдерской информации в своих интересах или в интересах третьих лиц;
- передавать третьим лицам или делать доступной для третьих лиц инсайдерскую информацию или основанную на ней информацию, за исключением случаев, предусмотренных законом;
- давать третьим лицам или делать доступной для третьих лиц инсайдерскую информацию или основанную на ней информацию за исключением случаев, предусмотренных законом;
- давать третьим лицам рекомендации о совершении сделок с ценными бумагами, основанными на инсайдерской информации.

Положения п.6.1. распространяются также на лиц, не являющихся инсайдерами, которым стала известна инсайдерская информация.

6.2. Инсайдерская информация представляется по мотивированному требованию органа государственной власти, иного государственного органа. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования инсайдерской информации и срок ее предоставления, если иное не установлено федеральными законами.

6.3. Инсайдеры в пределах своих полномочий обязаны принимать все зависящие от них меры к защите и недопущению неправомерного использования инсайдерской информации.

6.4. Сотрудники компании, уполномоченные осуществлять связь со средствами массовой информации, общественностью и акционерами в связи с исполнением служебных обязанностей, должны обеспечивать равную возможность всем заинтересованным лицам на одновременный доступ к раскрываемой инсайдерской информации о деятельности компании, а также должны принимать меры по незамедлительному опровержению недостоверной информации, которая выдается за инсайдерскую.

6.5. Обязательства инсайдеров в отношении инсайдерской информации остаются в силе в течение не менее одного года с момента устранения основания, по которому лицо признается инсайдером.

6.6. Обязательства инсайдеров в отношении конкретной инсайдерской информации прекращаются в момент раскрытия конкретной инсайдерской информации в порядке и с соблюдением требований законодательства Российской Федерации и настоящего Положения.

7. Ответственность за неправомерное использование инсайдерской информации.

7.1. Инсайдеры компании несут ответственность за неправомерное использование инсайдерской информации и могут быть привлечены к дисциплинарной, административной и гражданско-правовой ответственности в соответствии с законодательством Российской Федерации. К такой ответственности могут быть также привлечены и иные лица, не являющиеся инсайдерами, но распространяющие инсайдерскую информацию или совершающие операции с ценными бумагами компании.

7.2. Лица, допустившие несанкционированное распространение, совершение сделок или иное неправомерное использование инсайдерской информации, несут ответственность перед компанией за их виновные действия (бездействие). Компания вправе потребовать от инсайдеров, виновных в неправомерном использовании или распространении инсайдерской

информации, возмещения убытков, причиненных компании указанными неправомерными действиями.

8. Персональные данные.

8.1. Под персональными данными сотрудников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника, а также сведения о фактах, событиях и обстоятельствах жизни сотрудника, позволяющие идентифицировать его личность. Данные документы являются конфиденциальными.

8.2. К персональным данным относятся:

- сведения, содержащиеся в удостоверении личности;
- информация, содержащаяся в трудовой книжке;
- информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;
- документы воинского учета – при их наличии;
- информация об образовании, квалификации или наличии специальных знаний или подготовки;
- информация медицинского характера в случаях, предусмотренных законодательством;
- иная информация о сотруднике, содержащаяся в других документах, либо предоставленная им в устной форме.

8.3. Работодатель вправе получать и использовать только те сведения, которые необходимы для заключения с ним трудового договора.

9. Защита персональных данных сотрудников.

9.1. Все персональные данные сотрудника компании следует получать у него самого, при этом сотрудник обязан передавать работодателю достоверные документированные данные, а также своевременно сообщать об изменении своих персональных данных. Если персональные данные сотрудников возможно получить только у третьей стороны, то сотрудник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить сотруднику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа сотрудника дать письменное согласие на их получение.

9.2. Обработка персональных данных сотрудника компании может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия сотрудникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

9.3. При принятии решений, затрагивающих интересы сотрудника компании, работодатель не имеет права основываться на персональных данных сотрудника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

9.4. Доступ к персональным данным сотрудников разрешен только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

9.5. При передаче персональных данных сотрудника работодатель должен предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Данное положение не распространяется на обмен персональными данными в порядке, установленными федеральными законами.

9.6. В целях обеспечения сохранности и конфиденциальности персональных данных сотрудников компании все операции по их оформлению, формированию, ведению и хранению должны выполняться только лицами, осуществляющими данную работу в соответствии со своими должностными инструкциями.

10. Ответственность за разглашение информации, связанной с персональными данными сотрудника.

10.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных сотрудников компании, несут дисциплинарную, административную, гражданско-правовую ответственность в соответствии с федеральными законами.