Общество с ограниченной ответственностью
«_____»

УТВЕРЖДАЮ
Генеральный директор
ООО «_____»

_____ И. И. Иванов
подпись инициалы, фамилия

« 15 » февраля 2017 г.

ПОЛОЖЕНИЕ О КОНФИДЕНЦИАЛЬНОСТИ

СТО.ЛРК.04-2017 А

РАЗРАБОТАНО
Начальник лаборатории
разрушающего контроля
ООО «_____»

_____ В. В. Тихонов
подпись инициалы, фамилия

« 15 » февраля 2017 г.

Российская Федерация
2017

Оглавление

Конфиденциальная информация, в том числе коммерческая тайна, как правило, содержится в виде каких-либо документов – традиционных, бумажных, либо электронных. Эти источники информации могут являться объектами неправомерных посягательств и, следовательно, нуждаются в защите. Все документы в фирме делятся на три категории: входящие, исходяшие и внутренние. Первым шагом в обеспечении защиты информации является выявление из общей массы документов, содержащих ценную для фирмы коммерческую информацию. Процесс обеспечения сохранности информации в документах содержащих коммерческую тайну осуществляется в соответствии с основными стадиями “жизненного” цикла документа. Этими стадиями являются:

1 Получение (отправка) документа. Документ, поступающий в ЛРК, должен быть передан только начальнику ЛРК и зарегистрирован. Начальник ЛРК определяет непосредственного исполнителя по данному документу, имеющему допуск к этой категории документов, и адресует документ ему. Аналогичный порядок при отправлении документа – подготовка документа, подпись начальника, регистрация в специальном журнале и отправка.

2 Хранение документа. Все документы, содержащие конфиденциальную информацию, должны храниться в специально отведенных, закрывающихся помещениях, в запертых шкафах, столах или ящиках.

3 Использование документа. Система доступа сотрудников, не имеющих соответствующих прав по должности, к конфиденциальным документам должна иметь разрешительный характер. Каждая выдача таких документов регистрируется (расписываются оба сотрудника – и тот, кто берет документ и тот, кто его выдает) и проверяется порядок работы с ними (например, нарушением считается оставление данных документов на столе во время обеда, передача другим лицам, вынос за пределы служебных помещений).

4 Уничтожение документа. Конфиденциальные документы, утратившие практическое значение и не имеющие какой-либо правовой, исторической или научной ценности, срок хранения которых истек (либо не истек), подлежат уничтожению. Бумажные документы уничтожаются путем сожжения, дробления, превращения в бесформенную массу, а магнитные и фотографические носители уничтожаются сожжением, дроблением, расплавлением и др.

Контроль за соблюдением правил хранения и использования документов, содержащих конфиденциальную информацию, осуществляется с помощью проверок. Они могут быть как регулярными (еженедельными, ежемесячными, ежегодными), так нерегулярными (выборочными, случайными). В случае обнаружения нарушений составляется акт и принимаются меры, позволяющие в будущем предотвратить нарушения такого рода.

Следует контролировать не только документы, содержащие конфиденциальную информацию, но и бумаги с печатями, штампами, бланки. Бланк – лист бумаги с оттиском углового или центрального штампа, либо с напечатанным любым способом текстом (или рисунком), используемый для составления документа.

9 Компьютерная безопасность

В системе обеспечения безопасности и все большее значение приобретает обеспечение компьютерной безопасности. Это связано с возрастающим объемом поступающей информации, совершенствованием средств ее хранения, передачи и обработки. Перевод значительной части информации в электронную форму, использование локальных и глобальных сетей создают качественно новые угрозы конфиденциальной информации.

Источник данного вида угроз может быть внутренним (собственные работники), внешним (например, конкуренты), смешанным (заказчики – внешние, а исполнитель – работник фирмы). Как показывает практика, подавляющее большинство таких преступлений совершается самими работниками фирм.

Большую опасность представляют также компьютерные вирусы, то есть программы, которые могут приводить к несанкционированному воздействию на информацию, либо ЭВМ (системы ЭВМ и их сети), с теми же последствиями, для предотвращение этого в ЛРК используется безопасная локальная сеть (защищенная).

Угрозы компьютерным системам и компьютерной информации могут быть со стороны следующих субъектов:

– работники фирмы, использующие свое служебное положение (когда законные права по должности используются для незаконных операций с информацией);

работники фирмы, не имеющие права в силу своих служебных обязанностей, но, тем не менее, осуществившими несанкционированный доступ к конфиденциальной информации;

– лица, не связанные с фирмой трудовым соглашением (контрактом).

Способы защиты можно разделить на две группы – организационные и технические. Организационные способы защиты связаны с ограничением возможного несанкционированного физического доступа к компьютерным системам. Технические способы защиты предполагают использование средств программно-технического характера, направленных, прежде всего, на ограничение доступа пользователя, работающего с компьютерными системами фирмы, к той информации, обращаться к которой он не имеет права.

Направления технической защиты компьютерной системы:

– защита информационных ресурсов от несанкционированного доступа и использования – используются средства контроля включения питания и загрузки программного обеспечения, а также методы парольной защиты при входе в систему;

– защита информации в каналах связи и узлах коммутации – используются процедуры аутентификации абонентов и сообщений, шифрование и специальные протоколы связи;

– защита автоматизированных систем от компьютерных вирусов и незаконной модификации – применяются иммуностойкие программы и механизмы модификации фактов программного обеспечения

Действенным способом является ограничения несанкционированного доступа к компьютерным системам, также является регулярная смена паролей, особенно при увольнении работников, обладающих информацией о способах защиты.

В ЛРК выделяются следующие основные способы защиты информации:

1 Законодательный. Основан на соблюдении тех прав предпринимателя на конфиденциальную информацию, которые содержатся в российском законодательстве. При обнаружении нарушения прав предпринимателя как собственника, владельца или пользователя информации должно быть обращение в соответствующие органы (МВД, ФСБ, прокуратуру, суд) для восстановления нарушенных прав, возмещения убытков и т.п.

2 Физическая защита - охрана, пропускной режим, специальные карточки для посторонних, использование закрывающихся помещений, сейфов, шкафов и пр.

3 Организационный. Он включает:

– введение ответственности за соблюдение правил доступа и пользования конфиденциальной информацией;

– разделение информации по степени конфиденциальности и организация допуска к конфиденциальной информации только в соответствии с должностью или с разрешения руководства;

– соблюдение правил пользования информацией (не выносить за пределы служебных помещений, не оставлять без присмотра во время обеда, включить сигнализацию при уходе);

– наличие постоянно действующей системы контроля за соблюдением правил до-ступа и пользования информацией (контроль может быть визуальный, документальный и др.).

4 Технический. Используются такие средства контроля и защиты как сигнализирующие устройства, видеокамеры, средства идентификации, а также программные средства защиты компьютерных систем от несанкционированного доступа.

5 Работа с кадрами. Предполагает активную работу начальника ЛРК и специалиста по кадрам ООО «_____» по подбору и обучению персонала ЛРК.

10 Заключительные положения

Лист учета периодических проверок

Лист ознакомления

1 Область применения

1.1 Настоящие положение устанавливает требования к лаборатории разрушающего контроля ООО «_____» (далее ЛРК) и контролю выполнения законодательных актов Российской Федерации и подзаконных нормативных правовых актов по защите информации, обеспечению режима конфиденциальности проводимых работ, исключающего разглашение сведений, составляющих коммерческую или профессиональную тайну ООО «_____» (далее – предприятие).

1.2 Настоящие положение разработан в развитие требований ГОСТ ISO 9001-2011 (ГОСТ Р ИСО 9001-2015), ГОСТ Р ИСО/МЭК 17025-2009, критериев аккредитации, РК.ЛРК-1-2017 «Руководство по качеству лаборатории разрушающего контроля», СТО.ЛРК.02-2017 «Положение о лаборатории разрушающего контроля».

1.3 Действие настоящего положения распространяется на ЛРК и на ее всех должностных лиц. Требования положения являются обязательными.

2 Нормативные ссылки

2.1 Для ссылок на документацию внешнего происхождения используется первоначальное издание, актуальные версии (издания со всеми изменениями и дополнениями) контролируются и доступны в реестре актуальных версий документации. Для документации внутреннего происхождения используется издание без версии, актуальность версий контролируется и доступна в реестре актуальных версий документации.

В настоящем положении учтены положения документов, определенных в реестре актуальных версий документации, использованы ссылки на следующую организационную, нормативную документацию ЛРК и на документацию внешнего происхождения:

Федеральный закон Российской Федерации от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;

Постановление Правительства РСФСР от 05.12.1991 № 35 «О перечне сведений, которые не могут составлять коммерческую тайну»;

Федеральный закон РФ от 27.07.2006: № 152-ФЗ «О персональных данных»

ГОСТ ISO 9001-2011 «Системы менеджмента качества. Требования»;

ГОСТ Р ИСО 9001-2015 «Системы менеджмента качества. Требования»;

ГОСТ ИСО/МЭК 17025–2009 «Общие требования к компетентности испытательных и калибровочных лабораторий»;

РК.ЛРК-1-2017 «Руководство по качеству лаборатории разрушающего контроля»

СТО.ЛРК.02-2017 «Положение о лаборатории разрушающего контроля»