«УТВЕРЖДАЮ»
Директор ГБУ СО МО ЦСО
«Серпуховский городской дом ветеранов»
_____ С.В.Задорожнюк
«11» 01 2011 г.

Инструкция по защите конфиденциальной информации при обработке с помощью СВТ

1. Общие положения

Настоящая Инструкция разработана в соответствии с действующим законодательством РФ, должностными инструкциями и другими нормативно-правовыми документами.

Информация составляет конфиденциальные сведения в случае, если она имеет действительную или потенциальную ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации (Организация) принимает меры к охране ее конфиденциальности.

Конфиденциальную информацию (КИ), обрабатываемую с помощью средств вычислительной техники (СВТ), в ГБУ СО МО ЦСО «Серпуховский городской дом ветеранов» составляют:

- информация, содержащая данные о подопечных;
- персональные данные;
- технологическую информацию системы защиты информации, управления и администрирования.

Руководство ГБУ СО МО ЦСО «Серпуховский городской дом ветеранов» принимает меры по защите собственной КИ, а так же персональных данных, служебной тайны, коммерческой тайны и другой КИ в соответствии с Законодательством РФ.

Конфиденциальные сведения других юридических или физических лиц, переданные в ГБУ СО МО ЦСО «Серпуховский городской дом ветеранов» для выполнения работ или осуществления иной деятельности, и в отношении которых взяты обязательства о неразглашении и исключении неправомерного их использования, подлежат защите наравне с другой КИ ГБУ СО МО ЦСО «Серпуховский городской дом ветеранов»

Организация и проведение работ по защите КИ при ее обработке СВТ определяются действующими государственными стандартами, нормативными документами, а также организационно-распорядительными документами ГБУ СО МО ЦСО «Серпуховский городской дом ветеранов».

Подлежащей защите информацией, обрабатываемой с помощью СВТ, являются информационные ресурсы (ИР): данные, электронные документы, а также полученные при их обработке с помощью СВТ распечатки, печатные документы и электронные сообщения.

Защита КИ при обработке ее на СВТ обеспечивается системой организационных мер и средств защиты от несанкционированного доступа (НСД).

Обязательными условиями обработки КИ с помощью СВТ являются:

– определение перечня служебных помещений, в которых установлены СВТ, предназначенные для обработки и хранения КИ;

– определение круга лиц, допущенных к ознакомлению и обработке КИ;

– учет носителей информации, на которых хранится КИ;

– персональный допуск сотрудников к работам на СВТ, путем использования персональных идентификаторов и паролей;

– возможность идентификации всех лиц, обращающихся к конфиденциальным ИР;

– резервное копирование конфиденциальных ИР;

– возможность применения дополнительных мер защиты информации.

2. Создание конфиденциальных ИР

2.1. Регистрация конфиденциальных ИР

Все конфиденциальные ИР подлежат обязательной регистрации в журнале учета конфиденциальных ИР Организации, создаваемые путем сбора, ввода, приема информации, обрабатываемая конфиденциальная информация путем вывода (отображения, печати), передачи, записи, хранения, а также уничтожаемые в ИС ИР. Допускается ведение автоматизированного учета и регистрации с использованием СВТ с обязательным резервным копированием данных.

На носителях информации, содержащих КИ, проставляется штамп, в котором указывается наименование организации, регистрационный номер документа, гриф конфиденциальности, дата регистрации, количество файлов и общий занятый объем. Носители КИ подлежат инвентарному учету в журналах учета.

2.2. Ввод КИ

Ввод конфиденциальной информации с печатных документов и других источников должен осуществляться только на АРМ, предназначенных для обработки КИ, сотрудниками, имеющими допуск к работе с КИ. Создание конфиденциальных ИР путем объединения (агрегирования) информации из нескольких конфиденциальных ИР также является вводом и подлежит регистрации.

2.3. Прием КИ (ИР)

Прием КИ осуществляется путем получения ИР на носителях информации. При приеме КИ сверяются реквизиты носителя информации. В случае отсутствия на носителях файлов составляется акт в двух экземплярах, один из которых высылается отправителю. Ошибочно поступившие носители возвращаются отправителю.

Принимаемая КИ в любом виде подлежит обязательной антивирусной проверке.

3. Обработка

3.1. Вывод КИ

Вывод КИ осуществляется при печати ИР или отображении на устройствах вывода информации (мониторах, проекторах, экранах и т. д.). Вывод на печать конфиденциальных ИР должен быть явно разрешен руководителями Организации. Каждый печатный документ (в т. ч. черновик), подлежит регистрации. Вывод КИ разрешается только на АРМ, предназначенных для обработки КИ.

3.2. Передача и запись конфиденциальных ИР

Передача КИ осуществляется при пересылке (передаче) электронного документа, содержащего КИ с АРМ на любое другое СВТ. Запись конфиденциального ИР осуществляется при копировании, перемещении ИР с места исходного хранения на любой другой носитель информации или после внесения изменений в исходный ИР и записи на носитель. Передача КИ должна санкционироваться руководителем Организации. Передача КИ разрешается только на СВТ, предназначенные для обработки КИ.

Каждый вид передаваемых конфиденциальных ИР (файл, электронный документ, сообщение и т.д.) должен иметь состав реквизитов определенных требованиями к оформлению документов. При подготовке передаваемого ИР количество копий определяет исполнитель и руководитель, санкционирующий передачу ИР, а количество копий, адресаты, фамилия исполнителя и его телефон указываются на носителе.

Передача носителей, содержащих КИ, от одного сотрудника другому осуществляется с разрешения руководителя Организации, с отметкой в соответствующих журналах учета.

Запись конфиденциального ИР разрешается только на носители информации, предназначенные для хранения КИ, зарегистрированные и промаркированные в установленном порядке. Запрещается удалять (уничтожать) ИР на месте исходного хранения после копирования без прямого указания руководителя Организации и регистрации. Перемещение конфиденциального ИР (копирование без сохранения исходного ИР) должно сопровождаться необходимыми операциями по гарантированному уничтожению КИ на источнике.

Передача и запись конфиденциального ИР должна регистрироваться в журналах учета. Передача и запись КИ должна осуществляться только с АРМ, предназначенных для обработки КИ. При смене администратора, составляется акт приема-сдачи носителей, содержащих КИ, который утверждается руководителем Организации.

3.3. Хранение конфиденциальных ИР

Конфиденциальные ИР подлежат хранению только на выделенных для этой цели автономных АРМ и носителях информации. Носители информации, используемые при создании резервных копий конфиденциальных ИР, подлежат хранению так же, как и основные копии. Хранение конфиденциальных ИР производится в течение срока, определяемого в соответствующей организационно-распорядительной документации. Носители информации, содержащие конфиденциальные ИР, подлежат хранению в специально выделенном для этой цели сейфе.

4. Уничтожение конфиденциальных ИР

По истечении срока хранения, проведении мероприятий по ЗИ производится уничтожение конфиденциальных ИР. Данные операции производятся администратором. При снятии категории конфиденциальных ИР, они удаляются (уничтожаются) с носителей и АРМ-ов, предназначенных для хранения и обработки КИ.

Съемные носители КИ, при отсутствии необходимости их хранения, подлежат уничтожению. При уничтожении КИ составляется перечень всех носителей и АРМ, содержащих данный ИР, производится уничтожение данных ИР и составляется акт установленной формы.

5. Правила разграничения доступа

5.1. Субъекты доступа

Субъектами доступа к КИ АРМ являются:

– пользователи АРМ - сотрудники Организации, имеющие допуск к конфиденциальной информации; субъектом доступа - пользователем, может являться стороннее лицо, которому по решению руководителя Организации предоставлено разрешение ознакомления или обработки КИ на АРМ;

– администратор – сотрудник, имеющий допуск к КИ, осуществляющий администрирование и поддержание работоспособности АРМ и средств защиты информации, а также осуществляющий контроль выполнения требований по защите информации и исполнение организационно-распорядительных документов.

Субъектом доступа является как лицо, так и процесс в ИС, запущенный от лица данного субъекта.

5.2. Объекты доступа

Объектами доступа являются любые конфиденциальные ИР на носителях информации и в памяти ЭВМ.

5.3. Порядок и условия доступа

Организация работ по защите КИ, методическое руководство и контроль за эффективностью защиты информации возлагается на ответственного по защите информации. Ответственный по защите информации имеет административные права для управления АРМ.

Ответственный по защите информации несет персональную ответственность за создание необходимых условий по предотвращению несанкционированного ознакомления с конфиденциальными ИР и обеспечению их сохранности в Организации, при обработке их с помощью СВТ.

Субъекты доступа, независимо от служебного положения должны строго выполнять требования данной Инструкции, принимать меры по предотвращению утечки КИ и воздействия на КИ. Обязанности сотрудников Организации соблюдать требования настоящей Инструкции оговариваются при приеме на работу и закрепляются в приложении к Трудовому договору (в виде обязательства о неразглашении конфиденциальной информации).

С целью соблюдения принципа персональной ответственности за свои действия каждому субъекту доступа сопоставляется персональный уникальный идентификатор (логин, имя пользователя), под которым он регистрируется и работает на АРМ. Субъекту доступа в случае производственной необходимости могут быть сопоставлены несколько идентификаторов. Использование несколькими субъектами доступа одного и того же идентификатора для работы с КИ (группового имени) запрещено.

Предоставление доступа субъектам доступа к конфиденциальным ИР разрешается производить ответственному по защите информации. Субъекту под роспись сообщается идентификатор, пароль и передается персональный идентификатор.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на АРМ, обрабатывающих КИ и контроль за действиями субъектов возлагается на ответственного по защите информации.

Пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

– длина пароля - не менее 8 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

– субъект не имеет права сообщать пароль доступа другому субъекту.

Владельцы паролей должны быть ознакомлены с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольно-ключевой информации.

При наличии технологической необходимости в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. использования идентификаторов и паролей некоторых сотрудников в их отсутствие, идентификаторы и пароли предоставляются (ответственным сотрудником) с указания руководителя. При возвращении сотрудника к исполнению своих обязанностей, пароль изменяется в соответствии с вышеописанной процедурой.

Полная плановая смена паролей субъектов должна проводиться не реже одного раза в месяц. Внеплановая смена паролей или учетных записей субъекта производится в случае прекращения его полномочий (увольнение, переход на другую должность, в другое подразделение, сопровождаемое сменой допуска и прав доступа) или в случае компрометации пароля. Внеплановая смена паролей всех субъектов должна производиться в случае прекращения полномочий администратора.

Хранение сотрудником своих паролей (в печатном виде) и персональных идентификаторов допускается только в опечатанном конверте в сейфе.

6. Права субъектов доступа

6.1. Администратор имеет право:

– приостанавливать оказание информационных услуг, доступ к КИ субъектам в случаях аварийных ситуаций, компрометации парольно-ключевой информации и по указанию руководителя Организации;

– проверять наличия носителей у сотрудников;

– проводить контроль исполнения требований по защите информации и технологии обработки КИ.

6.2. ***Пользователи имеют право*** запрашивать информационные услуги, доступ к КИ и информацию о требованиях и правилах обработки КИ.

7. Обязанности субъектов доступа

Учет конфиденциальных ИР и носителей информации осуществляется администратором.

Проверка правил разграничения доступа, прав и полномочий доступа к конфиденциальной информации на АРМ, наличия носителей, содержащих конфиденциальную информацию, проводится один раз в год комиссией, назначаемой руководителем Организации. Результаты проверки оформляются актом.

Все субъекты обязаны:

– знать и выполнять требования настоящей Инструкции;

– знать состав Перечня сведений конфиденциального характера ООО «ВО АСТ»;

– хранить в тайне известную им КИ, информировать своего непосредственного руководителя о фактах нарушения порядка обращения с конфиденциальными ИР и носителями, и о попытках НСД к ним;

– соблюдать правила пользования конфиденциальными ИР и носителями, порядок их обработки и хранения;

– знакомиться только с той КИ, к которой получен доступ в силу исполнения прямых служебных обязанностей;

– о допущенных нарушениях установленного порядка работы, учета и хранения КИ, а также о фактах разглашения КИ представлять письменные объяснения.

8. Субъектам доступа запрещается

Администратору запрещается:

– предоставлять доступ в нарушении правил разграничения доступа и требований по защите информации;

– приостанавливать оказание информационных услуг, доступ к КИ без последующего незамедлительного уведомления субъекта доступа или руководителя подразделения сотрудника (при отсутствии возможности уведомления субъекта). Категорически запрещается производить регистрацию конфиденциальных ИР, ввод, прием, вывод КИ, передачу, запись и хранение конфиденциальных ИР на СВТ, не оснащенных средствами защиты информации, при отключенных или некорректно работающих средствах защиты информации.

– использовать КИ при ведении переговоров по незащищенным каналам связи;

– использовать КИ в личных целях;

– делать копии с конфиденциальных ИР и носителей, а также использовать различные технические средства для их записи без разрешения руководителя Организации;

– работать с КИ и носителями на дому;

– выносить носители информации, содержащие КИ, за пределы территории офиса Организации без разрешения руководителя Организации;

– сообщать устно или письменно кому бы то ни было (в том числе сотрудникам) КИ, если это не вызвано служебной необходимостью;

– делать записи, расчеты и заметки, содержащие КИ в личных тетрадях, блокнотах, на неучтенных носителях информации.

9. Ответственность субъектов доступа

Все субъекты доступа несут персональную ответственность за корректность и соответствие организационно-распорядительным документам проведения операций по ознакомлению, обработке КИ, простановке, снятию, зашифрованию и расшифрованию,

печать, ввод электронных документов (ИР), за сохранение в тайне и исключение утраты, подмены и разглашение парольно-ключевой информации, печатных документов (в т. ч. черновики), полученные при выводе конфиденциальных ИР. Ответственность субъектов доступа определяется действующим Законодательством РФ (в том числе УК РФ) и нормативно-правовыми документами Организации.