«УТВЕРЖДАЮ»
Директор
ООО «Реацентр Самарский»
Т.А. Гаврилова
«14» 04 2014 г.

ПОЛОЖЕНИЕ
о системе технической защиты персональных данных в ООО «Реацентр Самарский»

1. Общие положения

Целью, настоящего положения, является обеспечение безопасности объектов защиты персональных данных от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угрозы персональным данным.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности данных.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

2. Область действия

Требования настоящего Положения распространяются на всех сотрудников (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3. Система защиты персональных данных

Система защиты персональных данных (далее СЗПДН) строится на организационных мероприятиях для обеспечения безопасности персональных данных.

Организационные мероприятия должны включать:

- правовое основание для сбора персональных данных;
- определение ответственных лиц за соблюдением мер безопасности приказом по организации;
- защиту персональных данных, обрабатываемых без средств автоматизации;
- защиту персональных данных, обрабатываемых с применением средств автоматизации;
- защиту объектов от хищения;
- защиту съемных накопителей, содержащих персональные данные;
- вопросы уничтожения персональных данных.

В зависимости от уровня защищенности информационной системы персональных данных (ИСПДН) и актуальных угроз, СЗПДн может включать следующие технические средства:

- защиты от несанкционированного доступа к персональным данным;
- антивирусной защиты для рабочих станций пользователей и серверов;
- межсетевого экранирования;

4. Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- контроля отсутствия недекларированных возможностей;

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн.

Подсистема управления доступом должна осуществлять:

- идентификацию и проверку подлинности субъектов доступа при входе в операционную систему ИСПДн по идентификатору и паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;
- контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа.

Подсистема обеспечения целостности должна осуществлять:

- обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды.
- периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;
- наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

Межсетевое экранирование должно обеспечивать:

- идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- контроль целостности своей программной и информационной части;
- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

- регламентированное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления;
- предотвращение доступа не обладающего данным правом пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;
- возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной формы;
- контроль целостности программной и информационной части межсетевого экрана по контрольным суммам.

В информационных системах, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования), или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты.

Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений (СОВ).

5. Пользователи ИСПДн

В ИСПДн существует 2 группы пользователей, участвующих в обработке и хранении ПДн:

- администратор ИСПДн;
- пользователи ИСПДн.

Администраторы ИСПДн

Администратором является системный администратор ООО «Реацентр Самарский», ответственный за функционирование СЗПДн, обеспечение бесперебойного функционирования ИСПДн, создание резервных копий БД, назначается приказом директора.

Администратор обладает следующим уровнем доступа и знаний:

- обладает правами администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- имеет право доступа к конфигурированию технических средств сети, включая контрольные (инспекционные).

Администратор уполномочен:

- реализовывать политику безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты.

Администратор обладает правом копирования БД ИСПДн, и уполномочен на осуществление резервного копирования и хранение копий в порядке, установленном действующим законодательством и внутренними документами организации.

Пользователи ИСПДн.

Пользователеми ИСПДн являются работники ООО «Реацентр Самарский»: 1. Служба офис-менеджеров, 2. Врачи детского отделения неврологии и рефлексотерапии, 3. Кадровая служба, 4. Бухгалтерия. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПДн. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователь ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

6. Требования к персоналу по обеспечению защиты ПДн

Все работники, являющиеся пользователями ИСПДн, должны знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового работника кадровая служба и ответственный за конфиденциальную информацию, обязан организовать его ознакомление с должностной инструкцией и положением о защите персональных данных, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Работник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Работники, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (логинов и паролей) и не допускать несанкционированного доступа (НСД) к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Работники должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей.

Работники должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами третьим лицам.

При завершении работы с ИСПДн работники обязаны защитить рабочие места или терминалы с помощью блокировки паролем, если не используются более сильные средства защиты.

Работники должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на работников, которые нарушили принятые политику и процедуры безопасности ПДн.

Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и специалисту, ответственному за немедленное реагирование на угрозы безопасности ПДн.

7. Ответственность работников

Ответственный за обеспечение безопасности персональных данных несет личную ответственность за организацию работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных общества.

Ответственный за конфиденциальную информацию отвечает за все действия, совершенные от его имени и с его учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей, обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, за своевременное и полное исполнение обязанностей по формированию и хранению копий баз данных ИСПДн.

Пользователь ИСПДн, осуществляющий обработку ПДн, несет ответственность за все действия, связанные с неисполнением требований и правил по обработке ПДн в ИСПДн.

При нарушениях работниками ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.