ООО «МИРРА»
г. Санкт-Петербург
191025, Санкт-Петербург, ул. Марата, д2/73-75, лит.А, пом.1-Н
ИНН/КПП 7838000530/784001001
р/с 40702810455040001687
к/с 30101810500000000653
БИК 044030653
ПАО Сбербанк
ОГРН 1037851080145 ОКПО 15152193
т/ф 572-31-61

e-mail: mirramed@yandex.ru

Генеральный директор Рощенко Эрика Ласловна

Политика информационной безопасности ООО « МИРРА»

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 11 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», на основании:

«Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных Заместителем директора ФСТЭК России от 15.02.2008 г.,

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн Учреждения.

1 Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты Учреждения от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности сохранности персональных данных.

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 угрозу безопасности персональных данных.

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

Состав объектов защиты представлен в Перечне персональных данных, подлежащих защите.

2 Область действия

Требования настоящей Политики распространяются на всех сотрудников Учреждения (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, строится на основании:

- Отчета о результатах проведения внутренней проверки;

- Перечня персональных данных, подлежащих защите;

- Акта классификации информационной системы персональных данных;

- Модели угроз безопасности персональных данных;

- Положения о разграничении прав доступа к обрабатываемым персональным данным;

На основании этих документов определяется необходимый уровень защищенности персональных данных.

В организации составлен список используемых технических средств защиты, а также программного обеспечения участвующего в обработке персональных данных.

Система защиты персональных данных включает в себя:

- антивирусные средства для рабочих станций пользователей и серверов.

Список функций защиты включает в себя:

- управление и разграничение доступа пользователей;

- регистрацию и учет действий с информацией;

- обеспечение целостности данных;

- возможность производить обнаружений вторжений.

Список используемых средств поддерживается в актуальном состоянии. При изменении состава технических средств защиты, соответствующие изменения вносятся в Список и утверждаются руководителем ООО « МИРРА» или лицом, ответственным за обеспечение защиты ПДн.

Система антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ООО «МИРРА».

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;

- антивирусное сканирование;

- скрипт-блокирование;

- централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

- автоматизированное обновление антивирусных баз;

- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

- автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

Система анализа защищенности обеспечивает выявление уязвимостей, связанных с ошибками в конфигурации программного обеспечения, которые могут быть использованы нарушителем для реализации атаки на систему. Функционал системы реализован программными и программно-аппаратными средствами.

Система обнаружения вторжений обеспечивает выявление сетевых атак на элементы информационной системы персональных данных подключенные к сетям общего пользования и (или) международного обмена. Функционал системы реализован программными и программно-аппаратными средствами.

4 Пользователи ИСПДн

В ИСПДн в обработке и хранении ПДн участвуют:

- Администратор безопасности ИСПДн;

- Администратор ИСПДн ;

- Пользователи сети;

Все сотрудники ООО «МИРРА» , являющиеся пользователями ИСПДн, знают и строго выполняют установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности персональных данных.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами ООО «МИРРА», третьим лицам.

При работе с персональными данными сотрудники ООО «МИРРА» обязаны обеспечить отсутствие возможности просмотра данных третьими лицами с мониторов или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить мониторы или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники ООО «МИРРА» проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение, ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности персональных данных.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности персональных данных, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности персональных данных.

Генеральный директор ООО «МИРРА»

Рощенко Э.Л.

22.02.2022г.