УТВЕРДАЮ:
Глава Марьяновского муниципального
района Омской области
_____ А.И. Солодовниченко
«___» _____ 2013 г.

Порядок планирования и проведения проверок информационной безопасности в ИСПДн Администрации Марьяновского муниципального района Омской области

1. Общие положения.

Настоящий документ определяет порядок планирования и проведения проверок информационной безопасности от несанкционированного доступа, распространения, искажения и утраты в информационной системе персональных данных Администрации Марьяновского муниципального района. Проверка информационной безопасности осуществляется не реже одного раза в год. В ходе проверки осуществляется контроль эффективности внедренных на объекте защитных мер и средств защиты информации, в соответствии с требованиями предписаний на эксплуатацию технических средств и средств защиты информации. Обязательным является контроль:

- при вводе ИСПДн в эксплуатацию;
- после ремонта технических средств, входящих в состав ИСПДн и средств защиты информации;
- при изменении условий эксплуатации ИСПДн и размещения технических средств;

2. Контроль аппаратного обеспечения.

Контроль работоспособности аппаратных компонент ИСПДн, обрабатывающих персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию

оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности должны контролироваться постоянно в рамках работы администраторов соответствующих систем.

3. Контроль парольной защиты.

Контроль парольной защиты и контроль надежности пользовательских паролей проводится на основе «Инструкции по организации парольной защиты» и предусматривает:

- установление сроков действия паролей;
- периодическую проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

4. Контроль целостности.

Контроль целостности программного обеспечения включает следующие действия:

- проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;
- обнаружение дубликатов идентификаторов пользователей;
- восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

5. Контроль попыток несанкционированного доступа.

Предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы и специальных программных средств, и предусматривает:

- фиксацию неудачных попыток входа в систему в системном журнале;
- протоколирование работы сетевых сервисов;

- выявление фактов сканирования определенного диапазона сетевых портов, в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

6. Контроль производительности.

Контроль производительности ИСПДн, производится по обращениям пользователей, в ходе администрирования системы и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности системы.

7. Контроль защищённости системного и прикладного ПО.

Контроль защищённости системного и прикладного ПО производится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

Обзоры безопасности проводятся с целью проверки соответствия текущего состояния ИСПДн уровню безопасности, удовлетворяющему требованиям политики безопасности. Обзоры безопасности имеют целью выявление всех несоответствий между текущим состоянием ИСПДн и состоянием, соответствующем специально составленному списку для проверки.

Обзоры безопасности должны включать:

- отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;
- проверку содержимого файлов конфигурации на соответствие списку для проверки;
- обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);

- проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);
- проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;
- проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы. Информация об известных уязвимостях извлекается из документации и внешних источников. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т.е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то, с целью нейтрализации уязвимостей, необходимо либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

Внесение изменений в системное программное обеспечение осуществляется системным администратором, с обязательным документированием изменений в соответствующем журнале; уведомлением каждого сотрудника, кого касается изменение; выслушиванием претензий в случае, если это изменение причинило кому-нибудь вред; разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.