УТВЕРЖДАЮ
ректор МАЭУ
д.э.н., профессор Н.Н. Щебарова
«27» ноября 2009 г.

Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных

1. Общие положения

Мониторинг информационной безопасности и антивирусного контроля при обработке персональных данных осуществляется в режиме реального времени как на рабочих станциях (РС) пользователей, осуществляющих обработку персональных данных, так и на серверах электронной почты, доступа в Интернет и на которых они хранятся.

Мониторинг и антивирусный контроль осуществляется как с помощью специального программного обеспечения (ПО), так и при участии пользователей, осуществляющих обработку персональных данных на РС.

2. Обязанности пользователей информационной системы обработки персональных данных

2.1 Пользователи информационной системы должны производить мониторинг информационной безопасности и антивирусного контроля по следующим компонентам защиты:

- антивирусный контроль: мониторинг ПО, осуществляющего защиту от вредоносных программ и вирусов на РС, обрабатывающие персональные данные;
- несанкционированный доступ: мониторинг папок и файлов, паролей и попыток входа в систему другими пользователями.

2.2 При выявлении каких-либо ошибках в работе ПО и несанкционированного доступа необходимо незамедлительно сообщить Администратору информационной системы обработки данных.

3. Обязанности администратора информационной системы обработки персональных данных

3.1 Администратор информационной системы должен производить мониторинг информационной безопасности и антивирусного контроля по следующим компонентам защиты:

- аппаратное обеспечение: мониторинг работоспособности аппаратных компонент автоматизированных систем, обрабатывающих персональные данные (серверы, активное сетевое оборудование);
- парольная защита: мониторинг парольной защиты и контроль надежности пользовательских паролей (установление сроков действия паролей, проверка пользовательских паролей на количество символов и очевидность с целью выявления

слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств);

- несанкционированный доступ: предупреждение и своевременное выявление попыток несанкционированного доступа (фиксация 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);
- системный аудит: проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение;
- антивирусный контроль: настройка средств защиты от вредоносных программ и вирусов на РС и серверах автоматизированных систем, обрабатывающих персональные данные.

4. Действия пользователей и администратора информационной системы обработки персональных данных при выполнении мониторинга

4.1 Пользователь должен произвести следующие действия:

- мониторинг ПО, осуществляющего защиту от вредоносных программ: проверка автоматического запуска программ осуществляющих защиту РС от вредоносных программ и компьютерных вирусов при входе в систему.
- мониторинг несанкционированного доступа: проверка попытки входа или входа на РС какого-либо постороннего пользователя, не имеющего доступа к РС.

4.2 Администратор должен произвести следующие действия:

- мониторинг аппаратного обеспечения: контроль за наиболее существенными компонентами системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование);
- мониторинг парольной защиты: проверка пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей). Проверка сроков действия паролей и его смены пользователем;
- мониторинг несанкционированного доступа: фиксация неудачных попыток входа в систему и их регистрация 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;
- мониторинг системного аудита: проверка отчетов 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. Проверка содержимого файлов конфигурации. Обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов). Проверка прав доступа и других атрибутов системных файлов (команд, утилит и таблиц). Проверка правильности настройки механизмов аутентификации и авторизации сетевых сервисов. Проверка корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов);
- мониторинг антивирусного контроля: установка, настройка, обновления и проверка работоспособности средств защиты от вредоносных программ и вирусов на

рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные. При обнаружении зараженных вирусом файлов необходимо отключить РС от компьютерной сети, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения.

5. Ответственность пользователей и администратора системы обработки персональных данных

5.1 Пользователи и администратор несут ответственность за:

- ненадлежащее выполнение требований настоящей инструкции;
- не соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по мониторингу системы обработки персональных данных.