Министерство образования Кировской области

Кировское областное государственное бюджетное учреждение для детей-сирот и детей, оставшихся без попечения родителей, «Детский дом пгт Тужа»

Россия, 612200, Кировская область, п.г.т. Тужа, ул. Свободы, д. 6
Телефон: (83340) 2-23-07, Факс: 2-16-99
E-mail: tuzha_i-school@mail.ru

УТВЕРЖДАЮ
Директор КОГБУ для детей-сирот
«Детский дом пгт Тужа»
_____ / Л.И. Кошкина /
Приказ № 63-од от 28.05.2018 г.
М.П.

ИНСТРУКЦИЯ

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

Кировского областного государственного бюджетного учреждения для детей-сирот и детей, оставшихся без попечения родителей, «Детский дом пгт Тужа»

2018

1. Общие положения

Предметом настоящей Инструкции является порядок планирования и проведения мониторинга информационной безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации в Кировском областном государственном бюджетном учреждении для детей-сирот и детей, оставшихся без попечения родителей, «Детский дом пгт Тужа» (далее – Детский дом).

2. Мониторинг аппаратного обеспечения

Мониторинг работоспособности аппаратных компонентов автоматизированных систем, 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 (серверы, активное сетевое оборудование) должны контролироваться постоянно в рамках работы администраторов соответствующих систем.

3. Мониторинг парольной защиты

Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

Устранение сроков действия паролей (не более 3 месяцев);

Периодическую (не реже 1 раза в месяц) проверку с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

4.Мониторинг целостности программного обеспечения

Мониторинг 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.Мониторинг 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. Мониторинг производительности

Мониторинг производительности автоматизированных систем, обрабатывающих персональные данные, производится по обращениям пользователей, в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности систем.

7. Системный аудит

Системный аудит производится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности, тестирования системы, контроль внесения изменений в системное программное обеспечение.

Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, тому уровню безопасности, удовлетворяющему требованиям политики безопасности. Обзоры безопасности имеют целью выявление всех несоответствий между текущим состоянием системы и состоянием, соответствующим 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 системы. Информация об известных уяз-

вимостях 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 администраторами систем, обрабатывающих персональные данные, с обязательным документированием изменений в соответствующем журнале; уведомлением каждого сотрудника, кого касается изменение; выслушиваний 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.

8. Антивирусный контроль

Для защиты серверов и рабочих станций необходимо использовать антивирусные программы:

- Резидентные антивирусные мониторы, контролирующие подозрительные действия программ;
- Утилиты для обнаружения и анализа новых вирусов.

К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.

При подозрении на наличие невыявленных установленными средствами защиты заражений следует использовать другие антивирусные средства.

Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляются администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения рабочей станции должна быть выполнена антивирусная проверка.

Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

Антивирусный контроль рабочих станций должен проводится ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станциях занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной систе-

мы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещений.

Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т.п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.