Утверждена
приказом ТОГАПОУ
«Аграрно-промышленный колледж»
от 03.02.2014 № 16

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

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 колледжа.

2. Мониторинг аппаратного обеспечения.

Мониторинг работоспособности аппаратных компонент 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.

3.1. Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

3.1.1. Установление сроков действия паролей (не более 3 месяцев).

3.1.2. Периодическую (не реже 1 раза в месяц) 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. Мониторинг целостности.

4.1. Мониторинг целостности программного обеспечения включает следующие действия:

4.1.1. Проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы.

4.1.2. Обнаружение дубликатов идентификаторов пользователей.

4.1.3. Восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

5. Мониторинг попыток несанкционированного доступа.

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

5.1.1. Фиксацию неудачных попыток входа в систему в системном журнале.

5.1.2. Протоколирование работы сетевых сервисов.

5.1.3. 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.

7.1. Системный аудит производится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.
7.2. 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, соответствующем специально составленному списку для проверки.
7.3. Обзоры безопасности должны включать:

7.3.1. 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.

7.3.2. Проверку содержимого файлов конфигурации на соответствие списку для проверки. Обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов).

7.3.3. Проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц).

7.3.4. Проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов.

7.3.5. Проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

7.4. Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).
7.5. 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.
7.6. 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; 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.

8. Антивирусный контроль.

8.1. Для защиты серверов и рабочих станций необходимо использовать антивирусные программы:

8.1.1. Резидентные антивирусные мониторы, контролирующие подозрительные действия программ.

8.1.2. Утилиты для обнаружения и анализа новых вирусов.

8.2. К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.
8.3. При подозрении на наличие невыявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.
8.4. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные,

осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

8.5. 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.

8.6. 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).

8.7. Антивирусный контроль рабочих станций должен проводиться 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 системы 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 помещении.

8.8. 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.

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

8.10. На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее:

8.10.1. Осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер.

8.10.2. Проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

8.11. На серверах электронной почты необходимо применять антивирусное программное обеспечение, обеспечивающее проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна блокироваться. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

8.12. Необходимо организовать регулярное обновление антивирусных баз на всех рабочих станциях и серверах.

8.12. Администраторы систем должны проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которых распространяются вирусы. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

8.12.1. Отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения.

8.12.2. Немедленно сообщить о факте обнаружения вирусов непосредственному руководителю с указанием предположительного источника (отправителя, владельца и т.д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

9. Анализ инцидентов.

9.1. Если администратор системы, обрабатывающей персональные данные, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, то он должен установить:

9.1.1. Факт попытки несанкционированного доступа (НСД).
9.1.2. Продолжается ли НСД в настоящий момент.
9.1.3. Кто является источником НСД.
9.1.4. Что является объектом НСД.
9.1.5. Когда происходила попытка НСД.
9.1.6. Как и при каких обстоятельствах была предпринята попытка НСД.
9.1.7. Точка входа нарушителя в систему.
9.1.8. Была ли попытка НСД успешной.
9.1.9. Определить системные ресурсы, безопасность которых была нарушена.
9.1.10. Какова мотивация попытки НСД.

9.2. Для выявления попытки НСД необходимо установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях. Выявить подозрительную активность пользователей, проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго. Кроме того, необходимо проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

9.3. При анализе системных журналов администратору необходимо произвести следующие действия:

9.3.1. Проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени.
9.3.2. Проверить, не уничтожен ли системный журнал и нет ли в нем пробелов.
9.3.3. Просмотреть списки команд, выполненных пользователями в рассматриваемый период времени.
9.3.4. Проверить наличие исходящих сообщений электронной почты, адресованные подозрительным хостам.
9.3.5. Проверить наличие мест в журналах, которые выглядят необычно.
9.3.6. Выявить попытки получить полномочия суперпользователя или другого привилегированного пользователя.
9.3.7. Выявить наличие неудачных попыток входа в систему.

9.4. В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

9.4.1. Проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД.
9.4.2. Проверить, не уничтожен ли системный журнал и нет ли в нем пробелов.
9.4.3. Проверить наличие мест в журналах, которые выглядят необычно.
9.4.4. Выявить попытки изменения таблиц маршрутизации и адресных таблиц.
9.4.5. Проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

9.5. Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

9.5.1. Составить базовую схему того, как обычно выглядит система.
9.5.2. Провести поиск подозрительных файлов, скрытых файлов, имена файлов и каталогов, которые обычно используются злоумышленниками.
9.5.3. Проверить содержимое системных файлов, которые обычно изменяются злоумышленниками.
9.5.4. Проверить целостность системных программ.
9.5.5. Проверить систему аутентификации и авторизации.

9.6. В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

Специалист по защите информации В.М.Салычев