	ГОУВПО «Марийский государственный университет»
	Инструкция **СМК**
И СМК 6.2.2.01-2011	*Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных*

УТВЕРЖДАЮ

Ректор Марийского государственного университета

_____В.И.Макаров

«__» мая _____2011г

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

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

И СМК 6.2.2.01 - 2011

Версия 1.0 Изменение О

СОГЛАСОВАНО
Первый проректор - проректор по учебной работе,
представитель руководства по качеству

_____ В.А. Иванов

«_1_» _____мая_____ 2011г.

Йошкар – Ола 2011

Предисловие

1 РАЗРАБОТАНА Информационно-вычислительным центром ГОУВПО «Марийского государственного университета».

Руководитель разработки: Г.И. Миронов, проректор по учебной работе.

Разработчик: Курандин Л.В., начальник ИВЦ.

2 Утверждена и введена в действие_____от «25» мая 2011 г

Дата введения «25» мая_____2011 г

3 Введена впервые.

Содержание

1 Назначение и область применения

1.1 Настоящая инструкция является нормативным документом, устанавливающим единый порядок проведения мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных.

1.2 Требования инструкции обязательны для применения во всех подразделениях университета, непосредственно связанных с проведением мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных.

1.3 Особенности мониторинга информационной безопасности персональных данных в отдельных автоматизированных системах могут регулироваться дополнительными инструкциями.

1.4 Владельцем настоящей Инструкции по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных является проректор по учебной работе.

2 Нормативные ссылки

Инструкции по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных разработана в соответствии с требованиями следующих нормативных документов:

ПРИКАЗ ФСТЭК от 5 февраля 2010 г. N 58 «ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О МЕТОДАХ И СПОСОБАХ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ»;

Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ О персональных данных;

Трудовой кодекс РФ;

Иные федеральные нормативно-правовые акты в области защиты персональных данных и информации;

Положение «О защите персональных данных ГОУВПО «Марийский государственный университет»;

Приказы ректора (в области работы с персональными данными);

ГОСТ Р ИСО 9000-2001 СМК. Основные положения и словарь;

ГОСТ Р ИСО 9001-2008 СМК. Требования;

ДП СМК 4.2.3.01 Управление документацией.

3 Термины, определения, обозначения и сокращения

Сервер — техническое решение, которое предоставляет множеству компьютеров доступ к файлам, данным, ресурсам принтеров и факсов, а также многому другому. Сервером часто называют специальный компьютер (или оборудование), на котором работает серверное программное обеспечение.

Сетевое оборудование - устройства, необходимые для работы компьютерной сети, например: маршрутизатор, коммутатор, концентратор, патч-панель и др. Обычно выделяют активное и пассивное сетевое оборудование.

Взломщик паролей - это любая программа, которая может расшифровывать пароли или каким-либо другим способом снимать парольную защиту (например, расшифровать файл без знания правильного пароля).

Идентификатор [data name, identifier] - - в информатике специальное наименование, имя элементарных данных, массивов данных, программ или других объектов, которые запрашиваются, обрабатываются и выдаются на выход ЭВМ.

Информационная безопасность 1) комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с ее доступностью для всех авторизованных пользователей; 2) показатель, отражающий статус защищенности информационной системы. Отдельные сферы деятельности (системы государственного управления, банки, информационные сети и т. п.) требуют специальных мер обеспечения информационной безопасности и предъявляют особые требования к надежности функционирования в соответствии с характером и важностью решаемых задач. Достигается за счет реализации комплекса мероприятий и средств защиты, основанных на внутрифирменной политике безопасности и анализе рисков, допустимых для данной компании в конкретный период времени.

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Каталог — поименованная совокупность байтов на носителе информации, содержащая название подкаталогов и файлов.

Компьютерные вирусы (Computer viruses) - - программы или фрагменты программного кода, которые, попав на компьютер, могут вопреки воле пользователя выполнять различные операции на этом компьютере — создавать или удалять объекты, модифицировать файлы данных или программные файлы, осуществлять действия по собственному распространению по локальным вычислительным сетям или по сети Интернет.

Мониторинг — система периодического наблюдения за теми или иными объектами, сбора информации об их состоянии, осуществляемого с заданной периодичностью, цикличностью.

Несанкционированный доступ - доступ к программам и данным, который получают абоненты, которые не прошли регистрацию и не имеют права на ознакомление или работу с этими ресурсами.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу.

Протокол почтового офиса, почтовый протокол — протокол сети Интернет, позволяющий осуществлять динамический доступ в почтовый ящик сервера с рабочей станции.

Рабочая станция - абонентская система, работающая в составе компьютерной сети и специализированная на выполнение задач инженеров, экономистов, программистов и других специалистов.

Системный файл (System file) - - файл, содержащий один из модулей операционной системы или набор данных, которые она использует.

Утилиты специализированные программы, предназначенные для обслуживания и оптимизации работы системы, программы-помощники, решающие задачи, с которыми сама операционная система справиться не в состоянии.

Файл — наименование (имя) совокупности данных, в т. ч. документа на машиночитаемом носителе (например, дискете), основной элемент хранения данных в компьютере, позволяющий отличать эту совокупность данных от других, находить, изменять, удалять или выполнять с ней другие операции.

Электронная почта - сетевая служба, позволяющая пользователям обмениваться сообщениями или документами без применения бумажных носителей.

Обозначения

В настоящем документе приняты следующие сокращения:

ВПО - высшее профессиональное образование
ГОСТ Р - национальный стандарт Российской Федерации
И - инструкция
ИВЦ - информационно-вычислительный центр
ИСО - международная организация по стандартизации
МарГУ - Марийский государственный университет
МО - математического обеспечения
НСД - несанкционированный доступ
РК - Руководство по качеству
РФ - Российская Федерации
СМК - система менеджмента качества
СПС - сопровождения программных средств
ТиПР - телекоммуникаций и перспективных разработок
ТО - технического обеспечения
УБУФиП - управление бухгалтерского учета, финансов и прогнозирования
УМУ - учебно-методическое управление
ФЗ - федеральный закон
ФСТЭК - федеральная служба по техническому и экспертному контролю
ЭВМ - электронно-вычислительные машины
ЮО - юридический отдел

4 Описание процедуры

4.1 Общие положения

Настоящая инструкция определяет порядок планирования и проведения мониторинга информационной безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации ГОУВПО «Марийский государственный университет», далее Университет.

4.2 Виды мониторинга информационной безопасности

4.2.1 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.

4.2.2 Мониторинг парольной защиты

Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

- установление сроков действия паролей (не более 3 месяцев);
- 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).

4.2.3 Мониторинг целостности

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.

4.2.4 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.

4.2.5 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.

4.3 Порядок проведения системного аудита

Системный аудит 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 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.

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 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.

4.4 Порядок антивирусного контроля

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 не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

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.

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 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.

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.

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.

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

- осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;
- проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

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.

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

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:

- отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;
- немедленно сообщить о факте обнаружения вирусов непосредственному начальнику 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.

4.5 Порядок анализа инцидентов

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:

- факт попытки несанкционированного доступа (НСД);
- продолжается ли НСД в настоящий момент;
- кто является источником НСД;
- что является объектом НСД;
- когда происходила попытка НСД;
- как и при каких обстоятельствах была предпринята попытка НСД;
- точка входа нарушителя в систему;
- была ли попытка НСД успешной;
- определить системные ресурсы, безопасность которых была нарушена;
- какова мотивация попытки НСД.

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.

При анализе системных журналов администратору необходимо произвести следующие действия:

- 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;
- проверить не уничтожен ли системный журнал и нет ли в нем пробелов;
- просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;
- проверить наличие исходящих сообщений электронной почты, адресованные подозрительным хостам;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки получить полномочия суперпользователя или другого привилегированного пользователя;
- выявить наличие неудачных попыток входа в систему.

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

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

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

- составить базовую схему того, как обычно выглядит система;
- провести поиск подозрительных файлов, скрытые файлы, имена файлов и каталогов, которые обычно используются злоумышленниками;
- проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;

- проверить целостность системных программ;
- проверить систему аутентификации и авторизации.

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

5 Ответственность и полномочия

Ответственным за организацию разработки и введение инструкции в действие является проректор по учебной работе.

Распределение ответственности и полномочий подразделений и должностных лиц при выполнении процедуры по проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных приведено в таблице 1.

Таблица 1 Распределение ответственности полномочий

Операция (действие)	Ответственное лицо	Область ответственности
Мониторинг аппаратного обеспечения	Начальник ТО	Проведение работ по техническому обслуживанию оборудования
Мониторинг парольной защиты	Начальник отдела МО	Установление сроков действия паролей. Периодическую (не реже 1 раза в месяц) проверку пользовательских паролей на количество символов.
Мониторинг целостности	Начальник отдела МО	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.
Мониторинг попыток несанкционированного доступа	Начальник отдела МО	Фиксацию неудачных попыток входа в систему в системном журнале. Протоколирование работы сетевых сервисов. Выявление фактов сканирования определенного диапазона сетевых портов.
Мониторинг производительности	Начальник отдела МО Начальник отдела СПС	Администрирование систем и проведения профилактических работ.
Порядок проведения системного аудита	Начальник отдела МО Начальник отдела СПС	Проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.
Порядок антивирусного контроля	Начальник отдела МО Начальник отдела ТиПР	Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем.
Порядок анализа инцидентов	Начальник отдела МО	Выявления попытки НСД.

Лист согласования

Инструкцию разработал:

Начальник ИВЦ — 12.05.11 — Л.В. Курандин

Согласовано:

Проректор по учебной работе — 13.05.11 — Г.И. Миронов

Гл.бухгалтер, начальник УБУФиП — 19.05.11 — Н.В. Чеснокова

Начальник ЮО — 17.05.11 — Е.В. Лапина

Начальник УМУ — 20.05.11 — В.Н. Максимов

Начальник управления кадрами — 18.05.11 — Е.В. Маркова

Экспертиза проведена:

Начальник ОМКО — 20.05.2011г — Р.В. Босович

Лист регистрации изменений

Номер изменения	Номера листов			Основание для внесения изменений	Подпись	Расшифровка подписи	Дата	Дата введения изменения
	замененных	новых	аннулированных					