СОГЛАСОВАНО

Председатель профсоюзного комитета

МОУ «Общеобразовательный лицей № 17»

протокол № 7 от 20 октября 2011 года

_____/Барашнина Г.В/

УТВЕРЖДАЮ

Директор МОУ

«Общеобразовательный лицей № 17»

приказ №436 от 21 октября 2011 года

_____/Сахарова И.С./

И Н С Т Р У К Ц И Я

администратора безопасности

информационной системы персональных данных

МОУ «Общеобразовательный лицей № 17»

Содержание

1. Общие положения 3
2. Основные функции администратора безопасности 4
3. Права администратора безопасности 5
4. Ответственность администратора безопасности 5
5. Проведение мониторинга информационной безопасности и контроля при обработке персональных данных 5
   5.1. Мониторинг аппаратного обеспечения 5
   5.2. Мониторинг парольной защиты 5
   5.3. Мониторинг целостности 6
   5.4. Мониторинг попыток несанкционированного доступа 6
   5.5. Мониторинг производительности 6
6. Аудит информационной безопасности 6
7. Антивирусный контроль 7
8. Анализ инцидентов 9
9. Порядок действий при утрате или уничтожении съемных носителей персональных данных 10
10. Организационно–распорядительная, технологическая и эксплуатационная документация на информационную систему персональных данных 10

Приложения:

1. Приказ Учреждения «Об утверждении списка специалистов, доступ которых к персональным данным граждан необходим для выполнения функциональных обязанностей»
2. Приказ Учреждения «О назначении администратора информационной безопасности»
3. Акт обследования информационной системы персональных данных
4. Акт классификации информационной системы персональных данных
5. Технический паспорт информационной системы персональных данных, включая:
6. Перечень сведений о составе групп пользователей (Список пользователей)
7. Формуляр автоматизированной системы, входящей в состав информационной системы персональных данных
8. Перечень информационных ресурсов, содержащих персональные данные, подлежащих защите
9. Матрица доступа к информационным ресурсам
10. Акт о затирании остаточной информации, хранившейся на диске компьютера
11. Акт уничтожения съемных носителей
12. Журнал регистрации запросов субъектов персональных данных на предоставление доступа к своим персональным данным
13. Журнал учета проведения инструктажей пользователей информационной системы персональных данных по информационной безопасности
14. Журнал учета выдачи электронных идентификаторов
15. Журнал проверок на наличие компьютерных вирусов
16. Согласие на обработку персональных данных

1. Общие положения

1.1. Настоящая Инструкция администратора безопасности информационной системы персональных данных МОУ «Общеобразовательный лицей № 17» (далее – Инструкция) разработана в соответствии с Положением по организации защиты персональных данных в МОУ «Общеобразовательный лицей № 17».

1.2. Настоящая Инструкция включает основные обязанности, права и ответственность администратора безопасности – специалиста по обеспечению безопасности персональных данных, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации в информационных системах МОУ «Общеобразовательный лицей № 17» (далее – Учреждение), а также порядок проведения мониторинга информационной безопасности и контроля при обработке персональных данных.

1.3. Основная цель обеспечения информационной безопасности – предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в компьютерных и телекоммуникационных системах Учреждения.

1.4. Администратор безопасности информационной системы персональных данных назначается приказом директора Учреждения из числа наиболее квалифицированных специалистов, имеющих опыт работы по основной деятельности Учреждения или в области защиты информации и подчиняется непосредственно директору Учреждения.

В случае отсутствия в Учреждении квалифицированных специалистов директором Учреждения назначается ответственный за обеспечение информационной безопасности из числа специалистов информационного обеспечения.

В информационных системах персональных данных, до 2 класса защищенности включительно, допускается объединение ролей администратора системы и администратора безопасности.

Для работы в информационной системе персональных данных администратор безопасности должен быть допущен в установленном порядке к обработке персональных данных.

1.5. Администратор безопасности проводит свою работу согласно нормативным методическим документам Федеральной службы по техническому и экспортному контролю России, Федеральной службы безопасности России и иных уполномоченных законодательством органов в области обеспечения безопасности персональных данных.

1.6. Работа администратора безопасности проводится в соответствии с планами работ, утверждаемыми директором Учреждения.

1.7. В своей работе администратор безопасности руководствуется законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных, другими руководящими документами по обеспечению безопасности персональных данных.

1.8. Контроль за выполнением требований настоящей Инструкции осуществляется директором Учреждения.

2. Основные функции администратора безопасности

2.1. Проведение единой технической политики, организация и координация работ по обеспечению безопасности персональных данных в Учреждении или информационной системе персональных данных.

2.2. Проведение мероприятий по организации обеспечения безопасности персональных данных, включая участие в классификации информационных систем персональных данных.

2.3. Проведение мероприятий по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, в том числе:

– мероприятия по размещению, охране, организации режима допуска в помещения, в которых ведется обработка персональных данных;

– мероприятия по защите от несанкционированного доступа к персональным данным;

– мероприятия по закрытию технических каналов утечки персональных данных при их обработке;

– мероприятия по выбору средств защиты персональных данных при их обработке.

2.4. Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным или передачи их лицам, не имеющим права доступа к такой информации.

2.5. Своевременное обнаружение фактов несанкционированного доступа к персональным данным.

2.6. Недопущение воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование.

2.7. Обеспечение возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.8. Постоянный контроль за обеспечением уровня защищенности персональных данных.

2.9. Участие в подготовке информационной системы к оценке соответствия установленным требованиям или аттестации по выполнению требований обеспечения безопасности персональных данных.

2.10. Разработка организационных распорядительных документов по обеспечению безопасности персональных данных в Учреждении.

2.11. Организация в установленном порядке расследования причин и условий появления нарушений в безопасности персональных данных и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений.

2.12. Разработка предложений, участие в проводимых работах по совершенствованию системы безопасности персональных данных в Учреждении.

2.13. Проведение периодического контроля эффективности мер защиты персональных данных в Учреждении. Учет и анализ результатов контроля.

2.14. Организация повышения осведомленности руководства и работников Учреждения по вопросам обеспечения безопасности персональных данных.

2.15. Подготовка отчетов о состоянии работ по обеспечению безопасности персональных данных в Учреждении.

3. Права администратора безопасности

Администратор безопасности имеет право:

3.1. Запрашивать у работников Учреждения и получать необходимые материалы для проведения работ по вопросам обеспечения безопасности персональных данных.

3.2. Разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности персональных данных.

3.3. Готовить предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации.

3.4. Контролировать деятельность работников Учреждения в части выполнения ими требований по обеспечению безопасности персональных данных.

3.5. Вносить предложения директору Учреждения о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных.

3.6. Привлекать в установленном порядке необходимых специалистов из числа работников Учреждения для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных.

4. Ответственность администратора безопасности

Администратор безопасности несет персональную ответственность за:

– правильность и объективность принимаемых решений;

– правильное и своевременное выполнение приказов, распоряжений, указаний руководства Учреждения по вопросам, входящим в возложенные на него функции;

– выполнение возложенных на него обязанностей, предусмотренных настоящей Инструкцией;

– качество проводимых работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями;

– согласно действующему законодательству Российской Федерации за разглашение сведений ограниченного распространения, ставших известными ему по роду работы;

– соблюдение трудовой дисциплины, охраны труда.

5. Проведение мониторинга информационной безопасности и контроля при обработке персональных данных

5.1. 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.

5.2. 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 3 месяца) 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).

5.3. 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.

5.4. 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.

5.5. Мониторинг производительности

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

6. Аудит информационной безопасности

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

6.2. Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, установленному уровню безопасности, удовлетворяющему требованиям безопасности информации. Обзоры безопасности имеют целью выявление всех несоответствий между текущим состоянием системы и состоянием, соответствующим специально составленному списку для проверки.

6.3. 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).

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

6.5. Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы. Информация об известных уязвимостях извлекается из документации и внешних источников. Проверка конфигурации системы осуществляется 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.

6.6. Внесение изменений в системное программное обеспечение осуществляется администратором системы, в которой обрабатываются персональные данные, с обязательным документированием изменений в соответствующем журнале; уведомлением каждого работника, которого касается изменение; анализом претензий в случае, если это изменение привело к негативным последствиям; разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

7. Антивирусный контроль

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

- резидентные антивирусные мониторы, контролирующие подозрительные действия программ;

- утилиты для обнаружения и анализа новых вирусов.

7.2. К использованию в Учреждении допускаются только лицензионные антивирусные средства, закупленные у разработчиков (поставщиков) указанных средств, или сертифицированные свободно распространяемые антивирусные средства.

7.3. При подозрении на наличие невыявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

7.4. 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.

7.5. 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.

7.6. 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).

7.7. Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций 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.

Результаты полного антивирусного контроля автономных рабочих станций и обновления антивирусных баз должны отражаться в журнале учета (приложение 15).

7.8. 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.

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.

7.9. 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.

7.10. 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.

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

7.12. Администратор системы должен проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которые распространяются вирусы. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

- отключить от локальной сети рабочие станции, представляющие вирусную опасность, до полного выявления каналов проникновения вирусов и их уничтожения;
- немедленно сообщить о факте обнаружения вирусов непосредственному начальнику с указанием предполагаемого источника (отправителя, владельца и т.д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

8. Анализ инцидентов

8.1. В случае подозрения или получения сообщения о том, что информационная система, обрабатывающая персональные данные, подвергается атаке или уже была скомпрометирована, администратор системы 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.

8.2. 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 их области деятельности.

8.3. 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, адресованных подозрительным хостам;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки получить полномочия администратора (суперпользователя) или другого привилегированного пользователя;
- выявить наличие неудачных попыток входа в систему.

8.4. 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.

8.5. 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.

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

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

9. Порядок действий при утрате или уничтожении съемных носителей персональных данных

О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность директор Учреждения. В отношении работника, допустившего утрату, может быть проведено служебное расследование для привлечения к дисциплинарной ответственности.

На утраченные носители составляется акт.

Соответствующие отметки вносятся в журналы персонального учета съемных носителей персональных данных.

Съемные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт (приложение 10).

10. Организационно–распорядительная, технологическая и эксплуатационная документация на информационную систему персональных данных

В целях подготовки Заключения о соответствии информационной системы персональных данных установленным требованиям безопасности или аттестации по требованиям безопасности для создаваемых объектов информатизации, а также находящихся в эксплуатации, в Учреждении разрабатывается и утверждается организационно–распорядительная, технологическая и эксплуатационная документация, указанная в таблице 1.

Таблица 1. Формы документов

Прило–жение №	Документ, представляемый при проверке
1.	Приказ «Об утверждении списка специалистов, доступ которых к персональным данным граждан необходим для выполнения функциональных обязанностей»
2.	Приказ «О назначении администратора информационной безопасности»
3.	Акт обследования информационной системы персональных данных
4.	Акт классификации информационной системы персональных данных
5.	Технический паспорт информационной системы персональных данных, включая:
6.	Перечень сведений о составе групп пользователей (Список пользователей)
7.	Формуляр автоматизированной системы, входящей в состав информационной системы персональных данных
8.	Перечень информационных ресурсов, содержащих персональные данные, подлежащих защите
9.	Матрица доступа к информационным ресурсам
10.	Акт о затирании остаточной информации, хранившейся на диске компьютера
11.	Акт уничтожения съемных носителей
12.	Журнал регистрации запросов субъектов персональных данных на предоставление доступа к своим персональным данным
13.	Журнал проведения инструктажа по информационной безопасности
14.	Журнал учета выдачи электронных идентификаторов *При наличии программно–аппаратных средств защиты от НСД*
15.	Журнал проверок на наличие компьютерных вирусов
16.	Согласие на обработку персональных данных *Содержание формы может быть отражено в договоре с гражданином. Не требуется, если работа с персональными данными определена федеральными и областными законами. Основание обработки ПДн отражено в акте обследования, экспертном заключении*