ИНСТРУКЦИЯ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2020 год

Содержание

1. Термины и сокращения

АРМ - автоматизированное рабочее место.
ИСПДн - информационная система персональных данных.
ПО - программное обеспечение.
СКЗИ - средства криптографической защиты информации.
СЗИ - средства защиты информации.

2. Общие положения

2.1. Администратор информационной системы персональных данных (далее – Администратор) отвечает за обеспечение работоспособности элементов ИСПДн и средств защиты персональных данных.

2.2. Администратор назначается и освобождается от исполнения своих обязанностей распоряжением главы Администрации городского округа Электросталь Московской области и непосредственно подчиняется лицу, ответственному за организацию обработки персональных данных.

3. Должностные обязанности

3.1. Администратор обязан:

3.1.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и Приказов, регламентирующих порядок действий по защите информации.

3.1.2. Производить установку, настройку и своевременное обновление элементов ИСПДн:

а. программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);
б. аппаратных средств;
в. аппаратных и программных средств защиты.

3.1.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

3.1.4. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

3.1.5. В случае отказа работоспособности технических средств или программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.1.6. Информировать Администратора безопасности и лицо, ответственное за организацию обработки персональных данных о выявленных фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

3.1.7. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

3.1.8. Обеспечивать выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных

данных, проводятся организациями, имеющими соответствующую квалификацию. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения конфиденциальной информации без предварительного уничтожения данных администратором безопасности.

3.1.9. Присутствовать при выполнении технического обслуживания элементов ИСПДн сотрудниками сторонних организаций.

3.1.10. Принимать меры по реагированию, в случае возникновения внештатных и аварийных ситуаций, с целью ликвидации их последствий.

3.1.11. Все компоненты программного и аппаратного обеспечения ИСПДн должны использоваться администратором только в служебных целях. Использование их в других целях запрещается.

3.2. Все изменения конфигурации технических и программных средств осуществляются только после согласования планируемых изменений с администратором безопасности.

3.3. Любые изменения состава и конфигурации технических средств и программного обеспечения должны быть предварительно проанализированы на предмет их соответствия политике безопасности. Все добавляемые компоненты должны быть проверены на работоспособность, отсутствие вирусов и специальных вложений (вредоносных программ), а также отсутствие реализации опасных функций.

4. Антивирусный контроль

4.1. Для защиты рабочих станций необходимо использовать антивирусные программы:

а. резидентные антивирусные мониторы, контролирующие подозрительные действия программ;

б. утилиты для обнаружения и анализа новых вирусов.

4.2. К использованию допускаются только сертифицированные лицензионные средства защиты от вредоносных программ.

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

4.4. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется Администратором в соответствии с руководствами по установке применяемых средств антивирусной защиты.

4.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено Администратором на отсутствие вредоносных программ и компьютерных вирусов.

4.6. 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).

4.7. 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 файлов операционной системы и загружаемых файлов. В этом случае, полная проверка должна осуществляться не реже одного раза в месяц в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед.

4.8. 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.

4.9. Применять антивирусное программное обеспечение, обеспечивающее проверку всех сообщений электронной почты. В случае, если проверка сообщения электронной почты показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна блокироваться.

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

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

а. отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;

б. 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.

5. Планирование резервного копирования и восстановления информации

5.1. Для обеспечения целостности и доступности информационных систем персональных данных (баз данных ИСПДн, других необходимых данных) Администратор формирует «План резервного копирования информации».

5.2. «План резервного копирования информации» включает в себя:

а. периодичность резервного копирования;
б. тип резервного копирования;
в. параметры отчуждаемых носителей резервных копий;
г. места хранения отчуждаемых носителей резервных копий;
д. ФИО или должность сотрудника, ответственного за создание и/или хранение отчуждаемых носителей резервных копий.

5.3. Периодичность резервного копирования определяется на основании важности и частоты изменения информации.

5.4. Тип резервного копирования основан на анализе состояния атрибута «архивный» у файлов, содержащих информацию. Сброшенный атрибут автоматически восстанавливается операционной системой при изменении файла.

5.5. Типы резервного копирования подразделяются на:

а. полный (Normal), когда в контейнер резервного копирования архивируется вся подлежащая резервированию информация, при этом атрибут «архивный» у каждого файла сбрасывается;
б. дифференциальный (Differential), когда в контейнер резервного копирования архивируется вся подлежащая резервированию информация, у которой атрибут «архивный» у каждого файла установлен, при этом сам атрибут «архивный» в процессе копирования не изменяется;
в. инкрементальный (Incremental), когда в контейнер резервного копирования архивируется вся подлежащая резервированию информация, у которой атрибут «архивный» у каждого файла установлен, при этом сам атрибут «архивный» в процессе копирования сбрасывается;
г. ежедневный (Daily), когда в контейнер резервного копирования архивируется вся подлежащая резервированию информация, измененная в указанный день, независимо от состояния «архивного» атрибута копируемых файлов. Состояние атрибута «архивный» не изменяется.
д. копирующий (Copy), когда в контейнер резервного копирования архивируется вся подлежащая резервированию информация. Атрибут «архивный» не анализируется и не изменяется.

5.6. Периодичность и тип резервного копирования являются определяющими параметрами при определении скорости и трудоемкости как создания резервных копий, так и при восстановлении из них информации, поврежденной в результате аппаратного сбоя или реализации иной угрозы.

5.7. Выбор схемы резервного копирования определяется Администратором по согласованию с администратором безопасности по следующим параметрам:

а. критичность к скорости восстановления работоспособности информационной системы;
б. объем данных информационной системы;
в. частота изменения данных информационной системы;
г. периодичность создания резервных копий;

д. тип носителей резервных копий.

5.8. Рекомендуются следующие варианты:

а. Занимает больше места, дольше выполняется, но быстрее восстанавливается (используются два контейнера, первый и последний):
один раз в неделю в выходной – полная резервная копия;
ежедневно – дифференциальная копия;

б. Занимает меньше места, быстрее выполняется, но дольше восстанавливается (используются все созданные контейнеры от первого до последнего):
один раз в неделю в выходной – полная резервная копия;
ежедневно – инкрементальная копия;

в. Занимает очень много места, в сравнении с предыдущими вариантами, долго выполняется, но восстанавливается быстрее всех:
ежедневно – копирующая резервная копия.

5.9. Администратор, при составлении «Плана резервного копирования», должен проанализировать требования, предъявляемые к целостности и доступности данных конкретной информационной системы и выбрать наиболее подходящие периодичность и тип резервного копирования для данной информационной системы.

5.10. На этапе исполнения «Плана резервного копирования», Администратор обязан неукоснительно соблюдать сроки создания копий, анализировать состояние сменных носителей (количество сбойных участков, объем свободного места) и незамедлительно докладывать руководству обо всех произошедших или ожидаемых отклонениях от плана.

5.11. Администратор обязан разработать и согласовать со всеми соответствующими ответственными сотрудниками «Регламент восстановления поврежденных или утраченных данных информационной системы» (пример приведен в Приложении А).

5.12. В регламенте необходимо указать:

а. ФИО или должность сотрудника ответственного за содержание данных информационной системы (владелец ИСПДн – начальник соответствующего отдела);

б. способ связи с ответственным сотрудником, в том числе экстренный;

в. местонахождение «Плана резервного копирования» с отметками об исполнении;

г. место хранения носителей резервных копий;

д. ФИО или должность сотрудника ответственного за создание и/или хранение резервных копий;

е. порядок действий по определению признаков повреждения информационной системы, принятию решения на восстановление данных, предварительному извещению и получению санкции ответственных сотрудников и непосредственному восстановлению информации из резервных копий, включая предварительное копирование (при возможности) файлов с поврежденной информацией.

5.13. Администратор обязан не реже одного раза в месяц проверять работоспособность созданных резервных копий путем тестового восстановления данных на резервной системе. Отметка о проведении тестового восстановления проставляется в соответствующем поле «Плана резервного копирования».

5.14. Администратор обязан согласовывать любые изменения настроек резервного копирования с администратором безопасности и незамедлительно вносить изменения в

«План резервного копирования» и «Регламент восстановления поврежденных или утраченных данных информационной системы». После любых изменений настроек резервного копирования Администратор обязан проверить работоспособность созданных с измененными настройками резервных копий путем восстановления данных на резервной системе.

6. Мониторинг производительности

6.1. 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. Права Администратора

7.1. Администратор имеет право:

а. Требовать от сотрудников соблюдения правил работы со средствами защиты информации и СКЗИ, входящими в состав ИСПДн.

б. Осуществлять взаимодействие (давать необходимые рекомендации, проводить консультации, получать требуемые сведения) с сотрудниками по вопросам эксплуатации технических и программных средств с целью улучшения качества их работы, а также своевременного предупреждения аварийных ситуаций.

8. Ответственность Администратора

8.1. Администратор несет ответственность:

а. За неисполнение (ненадлежащее исполнение) своих обязанностей, предусмотренных настоящей инструкцией.

б. За совершенные в процессе осуществления своей деятельности правонарушения – в пределах определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

в. За причинение материального ущерба – в пределах, определенных действующим трудовым, уголовным и гражданским законодательством Российской Федерации.

Приложение А
Пример Регламента восстановления
поврежденных или утраченных данных ИСПДн

Регламент восстановления баз данных,
технических средств и программного обеспечения ИСПДн

В случае возникновения сбоев в работе компонентов ИСПДн, СЗИ, возникновения инцидентов ИБ, приведших к частичной или полной потере функциональности ИСПДн, Администратор ИСПДн обязан:

1. Незамедлительно уведомить сотрудников, выполняющих обработку персональных данных, о необходимости прекращения текущей работы, а также ответственного за организацию обработки персональных данных в Администрации городского округа Электросталь Московской области.
2. Проанализировать состояние аппаратных и программных технических средств, журналы событий и действия сотрудников непосредственно перед возникновением сбоя, определить причины сбоя и методы его устранения.
3. Перед проведением операций по восстановлению провести внеплановое резервное копирование баз данных, файлов пользователей и журналов безопасности.
4. Устранить причину сбоя. При необходимости переустановки операционные системы, СЗИ, антивирусные средства, прикладное ПО устанавливаются только с эталонных дистрибутивов. Порядок установки и восстановления программного обеспечения подробно описан в сопроводительной документации к этому ПО.
5. Произвести настройку переустановленного программного обеспечения в соответствии с эксплуатационной документацией. При необходимости восстановить базы данных, пользовательские файлы.
6. Протестировать все компоненты ИСПДн после восстановления.
7. Уведомить ответственных сотрудников о завершении работ по восстановлению компонентов ИСПДн.
8. Документально оформить факт потери функциональности ИСПДн с указанием даты, времени, причин сбоя, мер, предпринятых для восстановления, рекомендаций по предотвращению подобных сбоев.
9. В случае необходимости передачи аппаратных средств ИСПДн сторонней организации для ремонта произвести полное стирание персональных данных с передаваемых носителей.