Приложение № 9
к распоряжению Администрации
ЗАТО г. Железногорск
от 30.06.2014 № 132пр

ИНСТРУКЦИЯ
администратора безопасности информационных систем персональных данных
Администрации ЗАТО г. Железногорск

2013

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая инструкция является руководящим документом администратора безопасности, обеспечивающего безопасность персональных данных (далее – ПДн), обрабатываемых, передаваемых и хранимых в информационных системах персональных данных (далее – ИСПДн) «Бухгалтерия», «Гаражи и усадьбы», «Кадры», «СОТО», «АРМ «Административная комиссия», «АРМ «Договора», «АРМ «ЖФСИ», «АРМ «Общественная приемная», «АРМ «Спортсмены», «АРМ «Учет карточек профсоюза», «АРМ «Формирование изменений списков избирателей» Администрации ЗАТО г. Железногорск, настройку и функционирование средств защиты информации в соответствии приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», организационно-распорядительной документацией.

Требования администратора безопасности к пользователям ИСПДн, связанные с выполнением им своих функций, обязательны для исполнения всеми пользователями ИСПДн.

Администратор безопасности должен быть ознакомлен под подпись с настоящей инструкцией (лист ознакомления) и предупрежден о возможной ответственности за ее нарушение.

2 ФУНКЦИИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

В ходе исполнения своих обязанностей администратор руководствуется данной инструкцией и другими документами, регламентирующими защиту ПДн при их обработке в ИСПДн от несанкционированного доступа (далее – НСД) к ним, а также эксплуатационной документацией на установленные средства защиты информации (далее – СЗИ).

Администратор безопасности обеспечивает поддержку в работоспособном состоянии подсистем управления доступом пользователей к ресурсам ИСПДн, регистрации и учета информационных ресурсов ИСПДн, а именно:

- реализует полномочия доступа к ресурсам ИСПДн для каждого пользователя, допущенного к работе в ней и ознакомившегося с «Инструкцией пользователя ИСПДн», на основании «Положения о разрешительной системе доступа»;
- по согласованию с Заместителем Главы администрации ЗАТО г. Железногорск реализует полномочия доступа для сотрудников организации, оказывающих услуги аутсорсинга для Администрации ЗАТО г. Железногорск, а также контролирует их действия при их непосредственной работе в ИСПДн;
- своевременно проводит периодическую проверку работоспособности системы защиты от НСД к ней, а также принимает необходимые меры для восстановления системы защиты от НСД при сбоях;
- проводит генерацию и смену паролей пользователей для доступа в систему, в соответствии с действующей инструкцией по парольной защите. Периодически, по указанию ответственного за обработку ПДн в

Администрации ЗАТО г. Железногорск, уточняет список сотрудников (пользователей), допущенных к работе в ИСПДн, их права доступа и полномочия, с использованием которых осуществляется обработка персональных данных;

- по согласованию с ответственным за обработку ПДн регистрирует в ИСПДн (удаляет из ИСПДн) нового пользователя в соответствии с «Положением о разрешительной системе доступа».

Администратор безопасности контролирует целостность программно-аппаратной среды и хранимой и обрабатываемой информации в ИСПДн, а именно:

- следит за неизменностью программной и технической составляющей ИСПДн;
- своевременно принимает необходимые меры для восстановления ПДн, используя штатные средства операционных систем или специализированное программное обеспечение, позволяющее создавать резервные копии или архивирование необходимой информации, а также выясняет причины, приведшие к потере ПДн;
- проводит своевременное обновление антивирусных средств, а в случае обнаружения вирусов в ИСПДн, принимает необходимые меры в соответствии с «Инструкцией по организации антивирусного контроля».

Администратор безопасности осуществляет настройку и сопровождение подсистемы регистрации и учета действий пользователей при работе в ИСПДн, а именно:

- производит настройку операционной системы для обеспечения регистрации и учета входа (выхода) пользователей в систему (из системы) с регистрацией даты и временем входа и результатом попытки (успешной или неуспешной);
- проводит регулярный анализ соответствующих журналов СЗИ от НСД и операционной системы для выявления факта попыток несанкционированного доступа пользователей к защищаемым ресурсам ИСПДн или выявления фактов нарушения установленного порядка работы с персональными данными, представленного в «Описании технологического процесса обработки ПДн в ИСПДн».

Администратор безопасности контролирует размещение и состав технических средств ИСПДн, определенных в Техническом паспорте ИСПДн.

Внесение изменений в системное программное обеспечение осуществляется администратором безопасности ИСПДн, с обязательным документированием изменений в соответствующем журнале и уведомлением каждого пользователя ИСПДн, которого касается изменение.

Администратор безопасности проводит проверки соответствия текущего состояния ИСПДн уровню безопасности, удовлетворяющему требованиям организационной и распорядительной документации Администрации ЗАТО г. Железногорск (далее – проверка соответствия требованиям). Проверки соответствия требованиям производятся ежеквартально и в случаях нарушения

информационной безопасности ИСПДн. Они включают в себя проведение обзоров безопасности, активное и пассивное тестирование системы защиты ИСПДн, контроль внесения изменений в системное программное обеспечение.

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 информационную систему в обход системы защиты информации (с помощью систем анализа защищенности 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.

3 ПРАВА И ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИСПДн

На администратора безопасности возлагаются следующие обязанности:

- следить за сохранностью наклеек с защитной и идентификационной информацией на корпусах технических средств ИСПДн, состав которых определен в Техническом паспорте ИСПДн, а в случае их нарушения

информировать ответственного за обработку ПДн в Администрации ЗАТО г. Железногорск;

- своевременно информировать ответственного за обработку ПДн обо всех выявленных фактах попыток несанкционированного доступа пользователей к защищаемым ресурсам ИСПДн или фактов нарушения установленного порядка работы с ПДн, представленного в «Описании технологического процесса обработки ПДн в ИСПДн»;
- поддерживать и контролировать функционирование СЗИ, применяемых в ИСПДн, в соответствии с настройками, обеспечивающими необходимый уровень защищенности ПДн;
- поддерживать применяемые СЗИ в работоспособном состоянии и информировать ответственного за обработку ПДн в случае выхода их из строя (отклонения от нормального режима работы);
- не допускать к работе на рабочих станциях и серверах ИСПДн посторонних лиц;
- своевременно информировать ответственного за обработку ПДн обо всех компрометирующих действиях пользователей ИСПДн при работе в ИСПДн;
- совместно с ответственным за обработку ПДн принимать решение о прекращении обработки ПДн в ИСПДн при несанкционированном доступе (попытках) к ним или возникновении ситуаций, послуживших причиной возможной утраты ПДн;
- совместно с ответственным за обработку ПДн вести разбирательства по фактам нарушения порядка обработки ПДн, хранения носителей ПДн или нарушения порядка эксплуатации СЗИ;
- совместно с ответственным за обработку ПДн осуществлять работы по выбору, закупке и приемке нового программного обеспечения, средств защиты информации, технического оснащения, а также вести работы при подборе кадрового обеспечения организации в области защиты информации;
- обобщать результаты своей деятельности и готовить предложения по ее совершенствованию ответственному за обработку ПДн;
- следить за неизменностью условий функционирования и эксплуатации ИСПДн с последующим информированием ответственного за обработку ПДн в случае каких-либо изменений, руководствуясь настоящей инструкцией и другими нормативными документами по защите персональных данных в организации;
- подчиняться непосредственно ответственному за обработку ПДн или в случае его отсутствия Заместителю Главы Администрации ЗАТО г. Железногорск по общим вопросам Администрации ЗАТО г. Железногорск;
- проводить инструктаж пользователей ИСПДн по правилам работы с используемыми средствами защиты информации;
- вести журнал учета своей работы по обеспечению безопасности персональных данных при их обработке в ИСПДн (форма «Журнала работ администратора безопасности» приведена в приложении № 1);

4 ПОРЯДОК ДЕЙСТВИЙ ПРИ НАРУШЕНИЯХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В случае выявления фактов нарушений информационной безопасности администратор безопасности принимает меры, необходимые для предотвращения негативных последствий и информирует ответственного за обработку ПДн в ИСПДн и непосредственное руководство о факте нарушения и принятых мерах.

Администратор безопасности анализирует и устанавливает причины возникшего нарушения и принимает меры по предотвращению подобных нарушений в дальнейшем.

По факту нарушения администратор безопасности составляет служебную записку на имя Заместителя Главы Администрации ЗАТО г. Железногорск по общим вопросам Администрации ЗАТО г. Железногорск с указанием причин нарушения и принятых мер.

В случае создания комиссии по расследованиям причин нарушения администратор безопасности принимает участие в ее работе.

В случае, если администратор безопасности ИСПДн подозревает или получил сообщение о том, что ИСПДн подвергается атаке или уже была скомпрометирована, он должен установить:

- факт попытки несанкционированного доступа (НСД);
- продолжается ли НСД в настоящий момент;
- источник НСД;
- объект НСД;
- время осуществления попытки НСД;
- обстоятельства, при которых была предпринята попытка НСД;
- точку входа нарушителя в систему:
- успешность попытки НСД;
- определить системные ресурсы, безопасность которых была нарушена;

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.

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

- составить базовую схему системы;
- 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 проверка соответствия требованиям.

5 ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности несет всю полноту ответственности за качество и своевременность выполнения задач и функций, возложенных на него в соответствии с настоящей инструкцией и другими нормативными документами по защите ПДн в организации.

Персональные данные не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает администратора от взятых им обязательств по неразглашению сведений ограниченного распространения. За разглашение информации ограниченного распространения, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, сотрудник может быть привлечен к дисциплинарной или иной, предусмотренной законодательством ответственности.

Администратор безопасности, получивший доступ к ПДн, обязан хранить в тайне сведения ограниченного распространения, ставшие ему известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации.

В случае оставления занимаемой должности администратор безопасности обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, организации, ответственному за обработку ПДн.

Лист ознакомления

С настоящей инструкцией ознакомлен:

ФИО	Должность	Подпись	Дата

Приложение № 1
к инструкции администратора безопасности ИСПДн

Форма журнала работы администратора безопасности _____ при выполнении своих обязанностей:

Журнал начат «___» _____ 20__ г.	Журнал завершен «___» _____ 20__ г.
Должность:_____	Должность:_____
_____/ _____ ФИО Подпись	_____/ _____ ФИО Подпись

Журнал на ___ листах.

Дата проведения работ	Наименование работ		Наименование ресурса, где проводились работы	Отметка об успешном выполнении	Отметка о невыполнении с указанием причины			Подпись
	плановые	внеплановые			причина невыполнения	предпринятые действия	результат	
1	2	3	4	5	6	7	8	9