|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | Утверждаю | | |
|  | | Директор ООО «» | | |
|  |  | |  | \_\_\_\_\_\_\_\_\_ |
|  | | «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. | | |

**ИНСТРУКЦИЯ**

**администратора безопасности информационной системы персональных данных**

СОДЕРЖАНИЕ

[1. ОБЩИЕ ПОЛОЖЕНИЯ 3](#_Toc469221401)

[2. ИНСТРУКЦИЯ АДМИНИСТРАТОРА ИБ 3](#_Toc469221402)

[3. ПРАВА И ОТВЕТСТВЕННОСТЬ 7](#_Toc469221424)

# ОБЩИЕ ПОЛОЖЕНИЯ

* 1. Настоящая инструкция администратора системы защиты персональных данных (далее Инструкция) определяет основные права и обязанности администратора системы защиты персональных данных (далее Администратора ИБ) информационных систем п (далее – ИС) и автоматизированных систем (далее – АС) в ООО «».
  2. Администратор ИБ назначается приказом (или иным документом) директора ООО «».
  3. Администратор ИБ осуществляет деятельность в соответствии с нормативными и методическими документами Федеральной службы по техническому и экспортному контролю России, Федеральной службы безопасности России, Роскомнадзора иных уполномоченных законодательством органов в области обеспечения безопасности персональных данных.
  4. Назначение и освобождение от должности Администратора ИБ производится директором ООО «».
  5. Администратор ИБ назначается из работников ООО «», имеющих опыт работы по основной деятельности соответствующей организации или в области защиты персональных данных.
  6. Работа Администратора ИБ проводится в соответствии с планами работ, утверждаемыми директором ООО «».
  7. В своей работе Администратор ИБ руководствуется законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных, приказами и другими руководящими документами по обеспечению безопасности персональных данных.

# Инструкция администратора ИБ:

## Администратор ИБ должен использовать только сертифицированные средства защиты информации для исполнения своих функциональных задач.

## Администратор ИБ должен обеспечить доступ к обрабатываемым персональным данным пользователям ИС, согласно с их правами доступа.

## Администратор ИБ своевременно выявляет и предупреждает попытки несанкционированного доступа к персональным данным, путем фиксации неудачных попыток входа в систему в системном журнале, протоколирования работы сетевых сервисов, а также выявления фактов сканирования определенного диапазона сетевых портов, в короткие промежутки времени, с целью обнаружения сетевых анализаторов, изучающих ИС и выявляющих ее уязвимости.

## Администратор ИБ должен обеспечить возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

## Администратор ИБ принимает непосредственное участие в подготовке ИС к аттестации по выполнению требований обеспечения безопасности персональных данных.

## Администратор ИБ участвует в контрольных и тестовых испытаниях и проверках системы защиты персональных данных.

## Администратор ИБ обязан контролировать процесс резервирования и дублирования важных ресурсов ИС.

## Администратор ИБ участвует в приемке новых программных и аппаратных средств обработки персональных данных, проверяет их комплектацию и наличие сертификатов соответствия.

## Администратор ИБ анализирует данные журнала учета работы средств защиты персональных данных с целью выявления возможных нарушений требований защиты персональных данных. 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 привилегированного пользователя;
* выявить наличие неудачных попыток входа в систему.
* выявить попытки изменения таблиц маршрутизации и адресных таблиц;
* проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

## Администратор ИБ оценивает возможность и последствия внесения изменений в состав ИС с учетом требований по защите персональных данных, а так же подготавливать свои предложения.

## Администратор ИБ проводит мониторинг парольной защиты и контроль надежности пользовательских паролей, путем установки сроков действия паролей, а также периодической проверки пользовательских паролей на количество символов и очевидность, которые легко угадать или дешифровать с помощью специальных программных средств.

## Администратор ИБ должен запрещать и немедленно блокировать попытки изменения программно-аппаратной среды ИС без согласования порядка ввода новых (полученных из ремонта) технических средств и программного обеспечения, а так же средств защиты персональных данных.

## Администратор ИБ должен проводить системный аудит защищенности ИС и ее отдельных подсистем. Системный аудит производится ежеквартально и в особых ситуациях и проводятся с целью проверки соответствия текущего состояния ИС, требуемому уровню безопасности. Системный аудит должен 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;
* 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. Внесение изменений в системное программное обеспечение осуществляется Администратором, с обязательным документированием изменений в соответствующем журнале.

## Администратор ИБ проводит мониторинг производительности ИСПДн по обращениям пользователей, в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности систем.

## Администратор ИБ должен контролировать работоспособность аппаратных компонентов ИС, в том числе состояние системы защиты персональных данных, в процессе их администрирования, а также 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.

## Администратор ИБ должен периодически предоставлять директору Московской типографии – филиала ФГУП «Гознак» отчет о состоянии защиты ИС, в том числе информацию о нештатных ситуациях и допущенных пользователями нарушений установленных требований по защите персональных данных.

## Администратор ИБ оказывает помощь пользователям в части применения средств защиты от НСД и других средств защиты, входящих в состав системы защиты персональных данных.

## Администратор должен не допускать к работе на серверах ИС посторонних лиц.

## Администратор ИБ контролирует правильность применения пользователями ИС средств защиты.

## Администратор ИБ должен участвовать в расследовании причин и условий появления нарушений безопасности персональных данных и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений. В рамках расследования администратор 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 на АРМ пользователей не выполняются коды подозрительных программ и программ, не относящихся к его области деятельности.

## Администратор ИБ должен участвовать в проводимых работах по совершенствованию системы защиты персональных данных.

# ПРАВА И ОТВЕТСТВЕННОСТЬ

## Права Администратора ИБ

Администратор ИБимеет право:

* + 1. контролировать деятельность структурных подразделений соответствующей организации в части выполнения ими требований по обеспечению безопасности персональных данных;
    2. вносить предложения руководителю организации о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных;
    3. вносить предложения по совершенствованию уровня защиты ИСПДн;
    4. участвовать в разработке проектов организационных и распорядительных документов по обеспечению безопасности персональных данных.

## Ответственность Администратора ИБ

Администратор ИБнесет ответственность:

* + 1. за безопасность ИС, а также полноценное и правильное функционирование системы защиты ПДн;
    2. персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИС.