**УТВЕРЖДАЮ**

Должность

*подпись* ФИО

\_\_\_\_\_\_\_\_\_\_20\_\_г.

ИНСТРУКЦИЯ

администратора информационной безопасности

*наименование информационной системы*

## Общие положения

### Настоящая Инструкция определяет функции, права, обязанности и ответственность администратора информационной безопасности (далее – Администратор ИБ) информационной системы \_\_\_\_\_\_ в *наименование организации* (далее - Учреждение).

1. Администратор ИБ назначается приказом руководителя Учреждения и функционально подчиняется ему.
2. Администратор ИБ отвечает за обеспечение устойчивой работоспособности \_\_\_\_\_\_\_\_\_\_\_ Учреждения и средств защиты, применяемых в ней, а также безопасности информации, обрабатываемой и передаваемой при помощи средств вычислительной техники (СВТ) в \_\_\_\_\_\_\_\_\_\_\_.
3. Администратор ИБ организует выполнение мероприятий по защите информации на рабочих местах, подключенных к \_\_\_\_\_\_\_\_\_\_\_, обеспечивает сохранность защищаемой информации, настройку системы защиты информации от несанкционированного доступа (СЗИ НСД) в соответствии с разрешительной системой доступа пользователей к информационным ресурсам.
4. Администратор ИБ руководствуется требованиями нормативных документов Российской Федерации, нормативных актов Учреждения, настоящей Инструкцией, а также другими распорядительными документами в части, его касающейся.

1.6. В случае увольнения, Администратор ИБ обязан передать вновь принятому Администратору ИБ, либо сотруднику, исполняющему обязанности Администратора ИБ все носители защищаемой информации (диски, дискеты, распечатки с принтеров, модели, материалы, изделия и пр.), которые находились в его распоряжении в связи с выполнением им служебных обязанностей во время работы.

1.7. Администратор ИБ является ответственным должностным лицом Учреждения, уполномоченным по защите информации в \_\_\_\_\_\_\_\_\_\_\_ и поддержанию достигнутого уровня защиты \_\_\_\_\_\_\_\_\_\_\_ и ее ресурсов на этапах постоянной эксплуатации и модернизации.

1. **Функции администратора**

Администратор ИБ обязан:

1. Знать перечень установленных в \_\_\_\_\_\_\_\_\_\_\_ СВТ и перечень задач, решаемых их использованием.
2. Знать перечень рабочих мест, подключенных к \_\_\_\_\_\_\_\_\_\_\_, предназначенных для обработки и передачи информации, содержащей персональные данные и перечень задач, решаемых с их использованием.
3. Организовывать работу по предотвращению неправомерного доступа лиц к защищаемой информации.
4. Обеспечивать работоспособность СВТ \_\_\_\_\_\_\_\_\_\_\_ Учреждения, проводить организационно-технические мероприятия по их обслуживанию.
5. Контролировать установку и настройку элементов \_\_\_\_\_\_\_\_\_\_\_ и средств защиты информации, а также выполнять другие возложенные на него работы в соответствии с распорядительными, инструктивными и методическими материалами в части, его касающейся.
6. Контролировать установку, настройку и поддержание в исправном состоянии программных средств на рабочих местах, подключенных к \_\_\_\_\_\_\_\_\_\_\_.
7. Рассматривать целесообразность применения новых технологий для повышения эффективности функционирования \_\_\_\_\_\_\_\_\_\_\_ в Учреждении.
8. Выполнять своевременное обновление программного обеспечения элементов \_\_\_\_\_\_\_\_\_\_\_ и системы защиты персональных данных по мере появления таких обновлений. Осуществлять проверку целостности данных.
9. В случаях неисправности или нарушения целостности системы защиты информации \_\_\_\_\_\_\_\_\_\_\_ в Учреждении от несанкционированного доступа, выявления попыток несанкционированного доступа к защищаемой информации, немедленно прекратить работу, ограничить доступ в помещение и поставить в известность руководителя подразделения и ответственного за обеспечение безопасности персональных данных.
10. В случае выявления каких-либо неквалифицированных действий пользователей, не несущих в себе угроз для безопасности информации, поставить в известность об этом ответственного за обеспечение безопасности персональных данных, временно заблокировать возможность работы этого пользователя и организовать дополнительные занятия с ним.
11. В случае отказа работоспособности технических средств и программного обеспечения \_\_\_\_\_\_\_\_\_\_\_, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
12. Обеспечивать контроль за выполнением пользователями требований «Инструкции пользователя \_\_\_\_\_\_\_\_\_\_\_.
13. Осуществлять контроль за работой пользователей \_\_\_\_\_\_\_\_\_\_\_, выявление попыток НСД к защищаемым информационным ресурсам и техническим средствам \_\_\_\_\_\_\_\_\_\_\_Учреждения.
14. Осуществлять контроль за настройкой средств защиты, выполнять другие действия по изменению элементов \_\_\_\_\_\_\_\_\_\_\_.
15. Осуществлять учет всех защищаемых носителей информации, используемых в \_\_\_\_\_\_\_\_\_\_\_, с помощью их любой маркировки и с занесением учетных данных в специальный журнал (учетную карточку). Учтенные носители информации выдавать пользователям под роспись.
16. Осуществлять текущий, после сбоев и периодический контроль работы средств и систем защиты информации.
17. Осуществлять текущий контроль утвержденной технологии обработки защищаемой информации.
18. Выявление возможных каналов утечки защищаемой информации за счет несанкционированного доступа к информации в процессе деятельности и внесение предложений по их закрытию.
19. Периодически осуществлять тестирование всех функций системы защиты с помощью тестовых программ, имитирующих попытки НСД, при изменении программной среды и персонала \_\_\_\_\_\_\_\_\_\_\_.
20. Осуществлять контроль проверок информационной системы на отсутствие вредоносных программ.
21. В случае возникновения нештатных ситуаций (сбоев) немедленно докладывать ответственному за обеспечение безопасности персональных данных.
22. Участвовать в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности персональных данных.
23. Участвовать в проведении работ по восстановлению работоспособности средств и систем защиты информации при сбоях.
24. Проводить обучение персонала и пользователей вычислительной техники правилам работы с СВТ и средствами защиты информации.
25. Участвовать в разработке нормативных и методических материалов, связанных с функционированием СВТ и применением средств защиты информации, выполнением мероприятий по обеспечению защиты информации.
26. Регулярно анализировать работу любых элементов \_\_\_\_\_\_\_\_\_\_\_ для выявления и устранения неисправностей, а также для оптимизации ее функционирования.
27. Четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
28. Не допускать установку, использование, хранение и размножение в \_\_\_\_\_\_\_\_\_\_\_ программных средств, не связанных с выполнением функциональных задач.
29. При увольнении или переводе пользователей в другие подразделения оперативно изменять учетные реквизиты защиты: пароли, идентификаторы.
30. Генерировать ключи, личные идентификаторы, а также пароли для пользователей \_\_\_\_\_\_\_\_\_\_\_.
31. Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.
32. Не допускать к работе в \_\_\_\_\_\_\_\_\_\_\_ посторонних лиц.
33. Контроль доступа лиц в соответствии со списком сотрудников, допущенных к обработке персональных данных в \_\_\_\_\_\_\_\_\_\_\_.
34. Контроль за проведением смены паролей раз в 2 месяца для доступа пользователей к АРМ.
35. Требует прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.
36. Осуществляет настройку и сопровождение подсистемы регистрации и учета:
* вводит в базу данных системы защиты от НСД описания событий, подлежащих регистрации в системном журнале;
* проводит регулярный анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам.
1. Сопровождает подсистемы обеспечения целостности рабочего программного обеспечения (ПО):
* ведение копий программных средств защиты информации от НСД и контроль их работоспособности;
* контроль за отсутствием на магнитных носителях остаточной информации по окончании работы пользователей;
* контроль за периодическим обновлением антивирусных средств (баз данных), установленных на АРМ, контроль за соблюдением пользователями порядка и правил проведения антивирусного тестирования АРМ;
* поддержание установленного порядка и правил антивирусной защиты информации на АРМ;
* проводит контроль соответствия общесистемной программной среды эталону;
* обеспечивает поддержание установленного порядка и соблюдение требований инструкции по антивирусной защите.
1. **Ответственность администратора ИБ**.
2. На администратора ИБ возлагается персональная ответственность за качество и полноту проводимых им работ по обеспечению защиты информации в соответствии с его должностными обязанностями, предусмотренными настоящей инструкцией, другими инструктивными документами в соответствии с действующим трудовым законодательством Российской Федерации.
3. Администратор безопасности информации отвечает за соответствие настроек СЗИ от НСД.
4. Администратор ИБ несет ответственность за правонарушения, совершенные в процессе своей деятельности в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.
5. Администратор ИБ несет ответственность за разглашение сведений конфиденциального характера и другой защищаемой информации Учреждения в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.
6. **Права администратора ИБ**

Администратор ИБ имеет право:

1. Отключать любые элементы системы защиты персональных данных (СЗПД) при изменении конфигурации, при техническом обслуживании или при устранении неисправностей в установленном порядке.
2. В установленном порядке изменять конфигурацию элементов \_\_\_\_\_\_\_\_\_\_\_ и СЗПД.
3. Требовать от персонала и пользователей \_\_\_\_\_\_\_\_\_\_\_ соблюдения правил работы в ней, приведенных в «Инструкции пользователя \_\_\_\_\_\_\_\_\_\_\_.
4. Требовать от пользователей безусловного соблюдения установленной технологии обработки защищаемой информации и выполнения требований внутренних документов Учреждения, регламентирующих вопросы обеспечения безопасности и защиты информации.
5. Обращаться к пользователям с требованием о прекращении обработки информации в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования средств и систем защиты информации.
6. Вносить свои предложения по совершенствованию функционирования \_\_\_\_\_\_\_\_\_\_\_ в Учреждении.
7. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности в \_\_\_\_\_\_\_\_\_\_\_.

Приложение 1

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИИ В ИНСТРУКЦИИ
ЛИСТ № \_\_\_ регистрации изменений в Инструкции

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п.п. | Дата | Внесенное изменение | Основание (наименование, № и дата документа) | Кем внесено изменение (должность подпись) |
|  |  |  |  |  |

Лист ознакомления

с Инструкцией администратора информационной безопасности **\_\_\_\_\_\_\_\_\_\_\_**

информационных систем персональных данных

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Фамилия, инициалы сотрудника | Дата ознакомления | Расписка сотрудника в ознакомлении |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |