**ИНСТРУКЦИЯ АДМИНИСТРАТОРА**

безопасности значимого объекта критической информационной инфраструктуры «Система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Кемеровской области»

1. Общие положения
   1. Инструкция Администратора безопасности значимого объекта критической информационной инфраструктуры «Система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Кемеровской области» (далее – ЗОКИИ Система-112) (далее – Инструкция) определяет функции, права и обязанности Администратора безопасности значимого объекта по вопросам обеспечения информационной безопасности при подготовке и исполнении документов в ЗОКИИ Система-112.
   2. Администратор безопасности значимого объекта назначается из числа работников ГКУ «Агентство по защите населения и территории Кузбасса» приказом директора и обеспечивает правильность использования и нормальное функционирование установленной системы защиты ЗОКИИ Система-112.
   3. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима конфиденциальности и не исключает обязательного выполнения их требований.
   4. Администратор безопасности значимого объекта обладает правами доступа к любым программно-аппаратным средствам защиты информации (далее – СЗИ) на технических средствах пользователей. Он несет ответственность за реализацию принятой политики безопасности.
2. Должностные обязанности
   1. Администратор безопасности значимого объекта обязан:
      1. Осуществлять учет и периодический контроль за составом и полномочиями пользователей ЗОКИИ Система-112.
      2. Осуществлять оперативный контроль за работой пользователей ЗОКИИ Система-112, анализировать содержимое системных журналов средств вычислительной техники (далее – СВТ) и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование системных журналов СВТ и надлежащий режим хранения данных архивов.
      3. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых в ЗОКИИ Система-112 СЗИ.
      4. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных СВТ, обеспечивать и контролировать установку и настройку СЗИ.
      5. Не реже одного раза в месяц проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование).
      6. Управлять учётными записями пользователей, реализовывать правила разграничения доступа, а также осуществлять контроль соблюдения этих правил в соответствии с Политкой об управлении доступом субъектов доступа к объектам доступа значимого объекта критической информационной инфраструктуры «Система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Кемеровской области».
      7. Управлять идентификаторами (осуществлять создание, присвоение и уничтожение идентификаторов пользователей и устройств) и средствами аутентификации (аутентификационной информацией) внутренних пользователей в ЗОКИИ Система-112, обеспечивать соблюдение правил идентификации и аутентификации пользователей и устройств в соответствии с Правилами идентификации и аутентификации субъектов доступа и объектов доступа в значимом объекте критической информационной инфраструктуры «Система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Кемеровской области».
      8. Осуществлять контроль за хранением, выдачей, инициализацией, блокированием средств аутентификации и принятием мер в случае утраты и (или) компрометации средств аутентификации в соответствии с Правилами идентификации и аутентификации субъектов доступа и объектов доступа в значимом объекте критической информационной инфраструктуры «Система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Кемеровской области».
      9. Осуществлять контроль не реже одного раза в три месяца установленного (инсталлированного) в ЗОКИИ Система-112 программного обеспечения в соответствии с Правилами по ограничению программной среды в значимом объекте критической информационной инфраструктуры «Система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Кемеровской области».
      10. Осуществлять мониторинг и контроль применения мобильных технических средств в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в значимом объекте критической информационной инфраструктуры «Система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Кемеровской области» на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа ИС.
      11. Настраивать параметры журналов регистрации событий безопасности в соответствии с Правилами регистрации событий безопасности в значимом объекте критической информационной инфраструктуры «Система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Кемеровской области».
      12. Проводить мониторинг и анализ результатов регистрации событий безопасности и реагирование на них не реже одного раза в неделю.
      13. Управлять средствами антивирусной защиты в соответствии с Политикой по антивирусной защите значимого объекта критической информационной инфраструктуры «Система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Кемеровской области».
      14. Осуществлять контроль уровня защищенности информации, обрабатываемой в ЗОКИИ Система-112.
      15. Осуществлять контроль выполнения условий и сроков действия сертификатов соответствия на СЗИ и принятие мер, направленных на устранение выявленных недостатков.
      16. Обеспечивать сохранность СЗИ, эксплуатационной и технической документации к СЗИ, а также порядок обращения с СЗИ в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты информации, обрабатываемой с использованием средств автоматизации в соответствии с Политикой по порядку обращения со средствами защиты информации в значимом объекте критической информационной инфраструктуры «Система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Кемеровской области».
      17. Проводить не реже одного раза в три месяца контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в соответствии с Политикой идентификации и аутентификации пользователей в значимом объекте критической информационной инфраструктуры «Система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Кемеровской области».
      18. Своевременно и точно отражать изменения в организационно-распорядительных документах по управлению СЗИ, установленных на СВТ ЗОКИИ Система-112.
      19. Осуществлять поэкземплярный учет в соответствующем журнале:

* СЗИ (носителей дистрибутивов, системных блоков с установленными СЗИ);
* эксплуатационной и технической документации к СЗИ.
  + 1. Осуществлять хранение:
* носителей дистрибутивов СЗИ;
* лицензий и сертификатов на СЗИ.
  + 1. Не реже одного раза в месяц осуществлять проверки:
* состояния защищенности информационных ресурсов от сбоев в системе электропитания (система резервирования и автоматического ввода резерва);
* состояния линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатывающих устройств, оборудования распределительных шкафов).
  + 1. Проводить первоначальный, плановый и внеплановый инструктаж обслуживающего и эксплуатирующего персонала ЗОКИИ Система-112 по вопросам работы с СЗИ.
    2. Отвечать на вопросы обслуживающего и эксплуатирующего персонала ЗОКИИ Система-112, связанные с работой СЗИ.
    3. Составлять инструкции по работе с СЗИ.
    4. Докладывать руководству ГКУ «Агентство по защите населения и территории Кузбасса» об имевших место попытках несанкционированного доступа к информации и техническим средствам ИС.
    5. Участвовать в выявлении инцидентов информационной безопасности и реагировании на них.
    6. Управлять конфигурацией ЗОКИИ Система-112 и их системой защиты информации.

В ходе управления конфигурацией ЗОКИИ Система-112 и ее системы защиты информации осуществляются:

* поддержание конфигурации ЗОКИИ Система-112 и их системы защиты информации (структуры системы защиты информации ЗОКИИ Система-112, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации ЗОКИИ Система-112 и их системы защиты информации);
* управление изменениями базовой конфигурации ЗОКИИ Система-112 и их системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации ЗОКИИ Система-112 и их системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ЗОКИИ Система-112 и их системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ЗОКИИ Система-112 и их системы защиты информации, сохранение данных об изменениях базовой конфигурации ЗОКИИ Система-112 и их системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию ЗОКИИ Система-112 и их системы защиты информации;
* анализ потенциального воздействия планируемых изменений в базовой конфигурации ЗОКИИ Система-112 и их системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ЗОКИИ Система-112;
* определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ЗОКИИ Система-112 и их системы защиты информации;
* внесение информации (данных) об изменениях в базовой конфигурации ЗОКИИ Система-112 и их системы защиты информации в эксплуатационную документацию на систему защиты информации ЗОКИИ Система-112.
  + 1. В случае возникновения нештатных ситуаций и аварийных ситуаций принимать меры по реагированию в пределах функций и полномочий с целью ликвидации последствий. Оперативно докладывать вышестоящему руководству о случаях возникновения внештатных ситуаций и аварийных ситуаций. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов ЗОКИИ Система-112. Предпринимаемые меры по возможности согласовывать с вышестоящим руководством.

1. Права
   1. Администратор безопасности значимого объекта имеет право:
      1. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ЗОКИИ Система-112.
      2. Непосредственно обращаться к пользователям АРМ с требованием прекращения работы в ЗОКИИ Система-112 при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.
      3. В пределах своей компетенции сообщать своему непосредственному руководителю обо всех недостатках в работе ЗОКИИ Система-112 и их системы защиты.
      4. Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.
      5. Подписывать и визировать документы в пределах своих обязанностей в соответствии с настоящей Инструкцией.
      6. Получать доступ к информации, материалам, техническим средствам, помещениям, необходимый для надлежащего исполнения своих прав и обязанностей (в т.ч. вести мониторинг действий пользователей и обслуживающего персонала ЗОКИИ Система-112).
      7. Вносить свои предложения по совершенствованию мер защиты информации в ЗОКИИ Система-112.
2. Ответственность
   1. Администратор безопасности значимого объекта несет ответственность:
      1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, – в пределах, определенных действующим трудовым законодательством Российской Федерации.
      2. За правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.
      3. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

Лист ознакомления

с Инструкцией администратора безопасности значимого объекта критической информационной инфраструктуры «Система обеспечения вызова экстренных оперативных служб по единому номеру «112» на территории Кемеровской области»

| **№ п/п** | **ФИО** | **Должность** | **Дата**  **ознакомления** | **Подпись** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |