МЭРИЯ ГОРОДА ГРОЗНОГО

СОЬЛЖА - ГIАЛИН МЭРИ

Р А С П О Р Я Ж Е Н И Е

04.02.2021г. № 54

г. Грозный

Об утверждении инструкции по защите информации, не содержащей сведения, составляющие государственную тайну, в информационных системах Мэрии г. Грозного

В целях обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, и выполнения требований Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»:

1. Утвердить Инструкцию по защите информации, не содержащей сведения, составляющие государственную тайну, в информационных системах Мэрии г. Грозного согласно приложению.
2. Контроль за выполнением настоящего распоряжения оставляю за собой.
3. Настоящее распоряжение вступает в силу со дня его подписания и подлежит размещению на официальном сайте Мэрии г. Грозного.

Мэр города Грозного И.Н. Хаджимурадов

ПРИЛОЖЕНИЕ
к распоряжению Мэрии г. Грозного
от «26» 02 20 г. № 54

ИНСТРУКЦИЯ
по защите информации, не содержащей сведения, составляющие государственную тайну, в информационных системах Мэрии г. Грозного

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция по защите информации, не содержащей сведения, составляющие государственную тайну, в информационных системах Мэрии г. Грозного (далее – Инструкция) определяет основные функции, обязанности, права и ответственность лица, отвечающего за защиту информации, не содержащей сведения, составляющие государственную тайну, в информационных системах Мэрии г. Грозного (далее – Ответственный).

1.2. В своей деятельности Ответственный руководствуется настоящей Инструкцией, политикой в отношении обработки персональных данных в Мэрии г. Грозного, Положением по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в информационных системах Мэрии г. Грозного, локальными актами Мэрии г. Грозного (далее – Мэрия), регламентирующими процессы обеспечения защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация), действующим законодательством Российской Федерации в области защиты информации.

2. ОСНОВНЫЕ ФУНКЦИИ И ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ЗАЩИТУ ИНФОРМАЦИИ, НЕ СОДЕРЖАЩЕЙ СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ, В ИНФОРМАЦИОННЫХ СИСТЕМАХ

2.1. Функции Ответственного:

2.1.1. Обеспечение защиты информации на всех стадиях (этапах) создания, в ходе эксплуатации и вывода из эксплуатации информационной системы в соответствии с требованиями действующего законодательства Российской Федерации в области защиты информации от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию или носители такой информации.

2.1.2. Создание, эксплуатация и вывод из эксплуатации системы защиты информации информационной системы и, при необходимости,

2.1.2. Создание, эксплуатация и вывод из эксплуатации системы защиты информации информационной системы и, при необходимости, модернизация (развитие) системы защиты информации информационной системы.

2.1.3. Обеспечение выполнения организационных и технических мер защиты информации в рамках системы защиты информации информационной системы.

2.1.4. Анализ угроз безопасности информации в информационной системе.

2.1.5. Обеспечение должного уровня защищенности информации при ее обработке в информационной системе.

2.1.6. Координация и контроль деятельности лиц, обеспечивающих защиту информации в ходе эксплуатации информационной системы:

– сотрудников, ответственных за управление (администрирование) системой защиты информации информационной системы;

– сотрудников, ответственных за планирование и контроль мероприятий по защите информации в информационной системе;

– сотрудников, ответственных за выявление инцидентов и реагирование на них;

– сотрудников, которым разрешены действия по внесению изменений в конфигурацию информационной системы и ее системы защиты информации.

2.1.7. Содействие лицам, указанным в пункте 2.1.6, по вопросам защиты информации.

2.1.8. Обеспечение соответствия проводимых работ в части защиты информации технике безопасности, правилам и нормам охраны труда.

2.1.9. Взаимодействие с государственными органами Российской Федерации, регулирующими вопросы защиты информации, при проведении проверок, а также при обработке запросов указанных органов.

2.1.10. Взаимодействие с ответственным за обеспечение безопасности персональных данных при решении вопросов, связанных с созданием системы защиты информации информационной системы, ее эксплуатацией и выводом из эксплуатации (при обработке в информационной системе информации, содержащей персональные данные).

2.1.11. Обеспечение информирования и обучения пользователей информационной системы по вопросам обеспечения информационной безопасности и правилам работы в информационной системе.

2.1.12. Организация подготовки и периодической переподготовки (повышения квалификации) сотрудников Мэрии, непосредственно отвечающих за проведение работ по защите информации.

2.1.13. Организация и участие в мероприятиях по контролю за обеспечением уровня защищенности информации, содержащейся в информационной системе.

2.2. Ответственный обязан:

2.2.1. Знать и соблюдать требования действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности информации.

2.2.2. Знать состав, структуру, назначение и выполняемые задачи информационной системы, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку информации.

2.2.3. Знать состав, структуру и назначение систем защиты информации информационной системы, включая состав (количество) и места размещения ее элементов.

2.2.4. Не разглашать информацию ограниченного доступа, ставшую доступной в ходе исполнения должностных обязанностей.

2.2.5. Контролировать деятельность лиц, обеспечивающих защиту информации в ходе эксплуатации информационной системы.

2.2.6. Координировать внедрение и эксплуатацию средств защиты информации.

2.2.7. Периодически (в соответствии с планом мероприятий по защите информации в информационной системе) проводить анализ информационной системы на наличие известных уязвимостей (недостатков, слабостей), угроз безопасности информации в информационной системе.

2.2.8. Периодически (в соответствии с планом мероприятий по защите информации в информационной системе) проводить анализ изменения угроз безопасности информации в информационной системе и оценку возможных последствий от реализации угроз безопасности информации.

2.2.9. Принимать меры по устранению выявленных уязвимостей или по снижению возможностей их использования (эксплуатации).

2.2.10. Информировать пользователей информационной системы о появлении актуальных угрозах безопасности информации.

2.2.11. Доводить до пользователей информационной системы требования по защите информации, а также положения организационно-распорядительных документов по защите информации с учетом внесенных в них изменений.

2.2.12. Обучать пользователей информационной системы правилам эксплуатации средств защиты информации (при необходимости).

2.2.13. Проводить практические занятия и тренировки с пользователями информационной системы по блокированию угроз безопасности информации и реагированию на инциденты.

2.2.14. Периодически проводить контроль осведомленности пользователей информационной системы об угрозах безопасности информации и проверку уровня знаний пользователей информационной системы по вопросам обеспечения защиты информации.

2.2.15. Участвовать в мероприятиях по внутреннему контролю за обеспечением уровня защищенности информации, содержащейся в информационной системе.

2.2.16. Обеспечивать поддержание в актуальном состоянии локальных актов по защите информации.

2.2.17. Контролировать соблюдение требований законодательства Российской Федерации и локальных актов в области защиты информации пользователями (в том числе привилегированными) информационной системы.

2.2.18. Участвовать в реагировании, анализе и расследованиях инцидентов информационной безопасности.

2.2.19. Организовывать и участвовать в проведении периодического контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе.

2.2.20. Документировать процедуру и результаты контроля за обеспечением уровня защищенности информации.

2.2.21. Осуществлять организацию доработки (модернизации) системы защиты информации (при необходимости).

3. ПРАВА ОТВЕТСТВЕННОГО ЗА ЗАЩИТУ ИНФОРМАЦИИ, НЕ СОДЕРЖАЩЕЙ СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ, В ИНФОРМАЦИОННЫХ СИСТЕМАХ

3.1. Ответственный имеет право:

3.1.1. Знакомиться с локальными актами Мэрии, регламентирующими процессы обработки защищаемой информации.

3.1.2. Вносить предложения мэру города Грозного по совершенствованию существующей системы защиты информации.

3.1.3. Привлекать по согласованию с мэром города Грозного организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности», к работам по созданию, совершенствованию (модернизации, развитию) системы защиты информации и контролю за обеспечением уровня защищенности информации.

обеспечения безопасности защищаемой информации в информационной системе.

3.1.6. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности защищаемой информации.

3.1.7. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за организацию обработки персональных данных и ответственному за обеспечение безопасности персональных данных при их обработке в информационных системах.

4. ОТВЕТСТВЕННОСТЬ ЛИЦА, ОТВЕЧАЮЩЕГО ЗА ЗАЩИТУ ИНФОРМАЦИИ, НЕ СОДЕРЖАЩЕЙ СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ, В ИНФОРМАЦИОННЫХ СИСТЕМАХ

4.1. Ответственный в соответствии с возложенными на него обязанностями несет персональную ответственность за:

4.1.1. Реализацию политики в отношении обработки персональных данных в Мэрии.

4.1.2. Ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией.

4.1.3. Разглашение информации в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации.

4.1.4. Несоблюдение требований локальных актов Мэрии по защите информации, в пределах, установленных трудовым договором (служебным контрактом).