ГБПОУ Республики Марий Эл «Йошкар-Олинский строительный техникум»

СОГЛАСОВАНО
Председатель профкома
_____ Е.С. Бахтина
«__» _____ 20__г.

УТВЕРЖДАЮ
Директор ГБПОУ
Республики Марий Эл «ЙОСТ»
_____ И.С. Зяблицева
« » 2020г.

Инструкция ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.

1.Общие положения

1.1.Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – Ответственный) назначается приказом директора ГБПОУ Республики Марий Эл «Йошкар-Олинский строительный техникум».

1.2.Ответственный подчиняется директору ГБПОУ Республики Марий Эл «Йошкар-Олинский строительный техникум».

1.3.Ответственный в своей работе руководствуется нормативно-правовыми документами в области обеспечения безопасности персональных данных, локальными документами директору ГБПОУ Республики Марий Эл «Йошкар-Олинский строительный техникум».

1.4.Ответственный за обеспечение безопасности персональных данных является лицом, отвечающим за выявление инцидентов в информационной системе персональных данных и реагирование на них.

1.5.Рабочее место Ответственного должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к информационным системам персональных данных, а так же средствами контроля за техническими средствами защиты.

1.6.Ответственный осуществляет методическое руководство сотрудников информационных систем персональных данных, в вопросах обеспечения безопасности персональных данных.

1.7.Требования ответственного, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями информационных систем персональных данных.

1.8.Ответственный несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в информационных системах персональных данных, состояние и поддержание введенного режима безопасности персональных данных.

2.Должностные обязанности

2.1.Ответственный обязан:

2.1.1.Осуществлять установку, настройку и сопровождение технических средств защиты.

2.1.2.Участвовать в контрольных и тестовых испытаниях, проверках информационных систем персональных данных.

2.1.3.Участвовать в приемке и внедрении новых программных средств.

2.1.4.Обеспечить доступ к защищаемой информации пользователям информационных систем персональных данных согласно их правам доступа.

2.1.5.Вести контроль над процессом осуществления резервного копирования объектов защиты.

2.1.6.Осуществлять контроль над выполнением плана мероприятий по защите персональных данных.

2.1.7.Анализировать состояние защиты информационных систем персональных данных.

2.1.8.Контролировать неизменность состояния средств защиты их параметров и режимов защиты.

2.1.9.Контролировать физическую сохранность средств и оборудования информационных систем персональных данных.

2.1.10. Контролировать исполнение пользователями информационных систем персональных данных, правильность работы с элементами информационных систем персональных данных и средствами защиты.

2.1.11. Контролировать исполнение пользователями парольной политики.

2.1.12. Контролировать работу пользователей в сетях общего пользования и международного обмена.

2.1.13. Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.

2.1.14. Не допускать установку, использование, хранение и размножение в информационных системах персональных данных программных средств, не связанных с выполнением функциональных задач.

2.1.15. Не допускать к работе с персональными данными в информационных системах персональных данных посторонних лиц.

2.1.16. Осуществлять периодические контрольные проверки рабочих станций и тестирование

правильности функционирования средств защиты информационных систем персональных данных.

2.1.17. Оказывать помощь пользователям информационных систем персональных данных в части применения средств защиты и консультировать по вопросам защиты персональных данных.

2.1.18. Периодически представлять руководству отчет о состоянии защиты информационных систем персональных данных и о внештатных ситуациях на объектах информационных систем персональных данных и допущенных пользователями нарушениях установленных требований по защите персональных данных.

2.1.19. В случае отказа работоспособности технических средств и программного обеспечения информационных систем персональных данных, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.1.20. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

2.1.21. Участвовать в работе постоянно действующей экспертной комиссии.

2.1.22. Участвовать в служебных расследованиях для выяснения причин утечки или воздействия на обрабатываемую в информационных системах персональных данных информацию, компрометации паролей с целью выяснения величины нанесенного ущерба безопасности информации и выработки новых или совершенствования принятых технических и организационных мер по защите информации от реализации угрозы в будущем.

2.1.23. Участвовать в аттестации эксплуатируемых в ГБПОУ Республики Марий Эл «Йошкар-Олинский строительный техникум» информационных систем персональных данных на соответствие требованиям безопасности персональных данных.

2.1.24. При возникновении необходимости, организовывать и участвовать в мероприятиях, связанных с событиями вскрытия, опечатывания, модификации состава, ремонта и т.д. технических средств информационных систем персональных данных. Опечатывание корпусов технических средств информационных систем персональных данных.

Составление актов о вскрытии и опечатывании корпусов технических средств.

2.1.25. Проводить анализ воздействия изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение безопасности персональных данных.

2.1.26. Документально оформлять изменения в конфигурации информационной системы и системы защиты персональных данных.

2.1.27. Анализировать инциденты, в том числе, определять источники и причины возникновения инцидентов, а так же оценивать их последствия, принимать меры по устранению последствий инцидентов.

2.1.28. Планировать и принимать меры по предотвращению повторного возникновения инцидентов.

2.1.29. Вести журнал учета машинных носителей персональных данных .

2.1.30. Вести журнал учета средств защиты информации, эксплуатационной и технической документации к ним.

3.Права

3.1.Ответственный имеет право:

3.1.1. требовать от пользователей информационных ресурсов выполнения требований локальных нормативных актов по защите персональных данных, в том числе выполнение инструкций, а также проводить проверку соблюдения данных требований;

3.1.2. проводить служебные расследования по фактам нарушения установленных требований

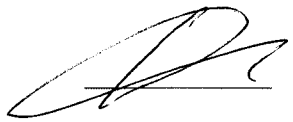
обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов информационных систем персональных данных;

3.1.3. вносить свои предложения по совершенствованию мер защиты в информационных системах персональных данных.

4.Ответственность

4.1.Ответственный за обеспечение безопасности персональных данных обязан соблюдать требования настоящей инструкции, а также других нормативных документов в области защиты информации. За разглашение персональных данных, а также за нарушение порядка работы с документами или носителями, содержащими такую информацию, может быть привлечен к дисциплинарной, уголовной, административной ответственности.

4.2.Ответственный за обеспечение безопасности персональных данных несет ответственность за все действия, совершенные от имени его учетной записи или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

Инструкцию разработал:  / М.В. Руденко /