ИНСТРУКЦИЯ

администратора информационной безопасности информационных систем муниципального бюджетного общеобразовательного учреждения города Кургана «Средней общеобразовательной школы № 56»

1 Общие положения

1.1 Настоящая инструкция разработана на основе:

- Методического документа «Меры защиты информации в государственных информационных системах», утвержденного Федеральной службой технического и экспортного контроля России 11 февраля 2014 года;
- Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2 Настоящий документ определяет основные обязанности, права и ответственность администратора информационной безопасности (далее - администратор ИБ) информационных систем (далее - ИС).

1.3 Администратор ИБ назначается приказом Директора муниципального бюджетного общеобразовательного учреждения города Кургана «Средней общеобразовательной школы № 56» (далее - Учреждение).

1.4 Администратор ИБ непосредственно подчиняется начальнику подразделения, в штате которого он состоит.

1.5 Администратор ИБ осуществляет контроль выполнения требований по защите ИС для соответствующего класса защищенности ИС.

1.6 Администратор ИБ обеспечивает решение вопросов информационной безопасности дополнительно к своим непосредственным обязанностям.

2 Обязанности администратора информационной безопасности

2.1 Администратор ИБ обязан:

- знать перечень установленных в Учреждении автоматизированных рабочих мест (далее - АРМ) и серверов, а также перечень задач, решаемых с их использованием;
- обеспечивать постоянный контроль за выполнением сотрудниками подразделения установленного комплекса мероприятий по обеспечению безопасности информации;
- контролировать целостность печатей (пломб) на АРМ и серверах ИС;
- в соответствии с принятой технологией работы в ИС проводить периодический анализ журналов безопасности средств защиты информации в ИС, а также архивирование и хранение этих журналов;
- немедленно сообщать руководству подразделения об имевших место в подразделении попытках несанкционированного доступа к информации и техническим средствам ИС, а также принимать необходимые меры по устранению нарушений;
- обеспечивать соблюдение сотрудниками Учреждения, эксплуатирующими ИС и ответственными за установку, модификацию и техническое обслуживание программного обеспечения и аппаратных средств ИС утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств ИС;
- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания АРМ и серверов ИС и отправке их в ремонт, контролировать затирание конфиденциальной информации на магнитных носителях;
- вести «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания АРМ и серверов, выполнения профилактических работ, установки

и модификации аппаратных и программных средств, защищенных АРМ и серверов»;

- присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИС подразделения;

- хранить технические паспорта и аттестационную документацию ИС, контролировать конфигурацию ИС и вести учет изменений аппаратно-программной конфигурации (архив документов, на основании которых были произведены данные изменения в ИС);

- осуществлять периодический контроль за правильностью использования съемных носителей информации в ИС;

- вести учет, хранить, осуществлять прием и выдачу персональных идентификаторов, осуществлять периодический контроль за правильностью использования персональных идентификаторов пользователями ИС;

- блокировать идентификатор пользователя через 90 дней неиспользования данного идентификатора;

- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИС и осуществления несанкционированного доступа к информации и техническим средствам ИС. При выявлении таковых сообщать о них руководству подразделения;

- проводить инструктаж сотрудников подразделения (пользователей средств вычислительной техники) по правилам работы с используемыми средствами и системами зашиты информации.

3 Права администратора информационной безопасности

• 3.1 Администратор ИБ имеет право:

- требовать от сотрудников подразделения - пользователей ИС соблюдения установленных технологий обработки информации и выполнения инструкций по обеспечению безопасности и защите персональных данных, обрабатываемых в ИС;

- инициировать проведение служебных расследований по фактам

нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИС;

- обращаться к руководителю подразделения с требованием прекращения работы пользователя в ИС при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности, давать своему непосредственному начальнику свои предложения по совершенствованию мер защиты.

4 Ответственность администратора информационной безопасности

4.1 На администратора ИБ возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты информации в Учреждении.

4.2 Администратор ИБ несет ответственность по действующему законодательству Российской Федерации за разглашение конфиденциальных сведений, ставших известными ему в ходе выполнения своих трудовых обязанностей.