

2.2.6. Контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК.

2.2.7. Контроль пользования Интернетом.

1. **Обязанности ответственных за информационную безопасность**

3.1.Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных на них обязанностей. Немедленно докладывать заведующему Учреждения о выявленных нарушениях и несанкционированных действиях пользователей и сотрудников, а также принимать необходимые меры по устранению нарушений.

3.2.Совместно с программистами принимать меры по восстановлению работоспособности средств и систем защиты информации.

3.3.Проводить инструктаж сотрудников и пользователей ПК по правилам работы с используемыми средствами и системами защиты информации.

3.4.Создавать и удалять учетные записи пользователей.

3.5.Администрировать работу сервера ЛВС (локальная вычислительная сеть), размещать и классифицировать информацию на сервере ЛВС.

3.6.Устанавливать по согласованию с заведующим Учреждения критерии доступа пользователей на сервер ЛВС.

3.7.Формировать и представлять пароли для новых пользователей, администрировать права пользователей.

3.8.Отслеживать работу антивирусных программ, проводить полную проверку компьютеров на наличие вирусов.

3.9.Выполнять регулярно резервное копирование данных на сервере, при необходимости восстанавливать потерянные или поврежденные данные.

3.10. Сообщать незамедлительно заведующему Учреждения о выявлении случаев несанкционированного доступа в Интернет.

1. **Права ответственных лиц за информационную безопасность**

4.1.Требовать от сотрудников и пользователей компьютерной техники безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения и электронных платежей.

4.2.Готовить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов.