

УТВЕРЖДАЮ  
Директор ГБУ  
«Сормовский дом-интернат»  
Т.Ю. Фадеева  
21 февраля 2018г.

## **ИНСТРУКЦИЯ ДЛЯ СОТРУДНИКОВ ГБУ «СОРМОВСКИЙ ДОМ-ИНТЕРНАТ» ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

### **1. ОБЩИЕ ТРЕБОВАНИЯ**

При работе с информационными ресурсами Учреждения каждый сотрудник обязан:

- обеспечивать, исходя из своих возможностей и специальных обязанностей по обеспечению безопасности информации, защиту от несанкционированного доступа к информации, к которой он имеет санкционированный доступ в силу своих служебных обязанностей;
- ни в какой форме не участвовать в процессах несанкционированного доступа к информации, принадлежащей другим сотрудникам и службам;
- ни в какой форме не использовать ставшую ему известной в силу исполнения своих функциональных обязанностей информацию не по прямому назначению;
- при нарушении установленных правил доступа другими сотрудниками сообщать об этом непосредственному начальнику либо администратору информационной безопасности.

Ремонтные и профилактические регламентные работы должны производиться только уполномоченными лицами по согласованию с руководителем подразделения, в котором установлено компьютерное оборудование. Снятие, перенос, модификации аппаратной конфигурации осуществляется только уполномоченными лицами.

### **2. РАБОТА В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ**

При работе в автоматизированной информационной системе Учреждения пользователь обязан:

- сохранять в тайне пароли доступа к системе (системам);
- надежно хранить физические ключи (идентификаторы) доступа;

- при случайном получении (сбой механизмов защиты, аварии, небрежность персонала и др.) доступа к чужой конфиденциальной информации прекратить какие-либо действия в системе и незамедлительно сообщить администратору ИБ;
- сообщать администратору ИБ об известных каналах утечки, способах и средствах обхода или разрушения механизмов защиты.

При работе в автоматизированной информационной системе Учреждения пользователю запрещается:

- записывать в любом доступном виде или произносить вслух известные пользователю пароли;
- регистрироваться и работать в системе под чужим идентификатором и паролем;
- передавать идентификаторы и пароли кому бы то ни было;
- оставлять без контроля рабочее место в течение сеанса работы;
- позволять производить любые действия с закреплённым за пользователем комплектом программно-аппаратных средств другим лицам;
- несанкционированно изменять или уничтожать данные или программы в сети или на внешних (отчуждаемых) носителях;
- использовать компьютерную технику в нерабочее время не по прямому назначению;
- игнорировать системные сообщения и предупреждения об ошибках;
- несанкционированно устанавливать на автоматизированные рабочие места любые дополнительные программные и аппаратные компоненты и устройства;
- копировать на съёмные носители любое программное обеспечение и файлы данных;
- использовать для передачи информации ограниченного доступа не предназначенные для этого средства и каналы связи.

При нарушениях правил, связанных с информационной безопасностью, пользователь несет ответственность, установленную действующим законодательством Российской Федерации. Пользователь несет ответственность за все действия, совершенные от имени его идентификатора, учетной записи или логина, если не доказан факт несанкционированного использования таковых.