УТВЕРЖДАЮ
директор ГАУ ДО РДОЦТ
Рахматуллин Р.Н.
«19» 06 2024 г. №

ИНСТРУКЦИЯ
о порядке пользования вычислительной и оргтехникой, программным обеспечением и работы в информационной вычислительной сети

1. Общие положения

1.1. Настоящая Инструкция определяет порядок пользования вычислительной техникой, программным обеспечением и работы в информационной вычислительной сети ГАУ ДО РДОЦТ.

1.2. Компьютерные и телекоммуникационные ресурсы и службы включают в себя следующее: многофункциональные серверы, рабочие станции, автономные компьютеры, мобильные компьютеры и другое оборудование, программное обеспечение, а также внутренние и внешние сети связи (сеть Интернет, системы электронной почты и т.д.), к которым прямо или косвенно обращаются вычислительные устройства ГАУ ДО РДОЦТ.

1.3. Директор ГАУ ДО РДОЦТ назначает в соответствие с установленными правилами лицо, ответственное за информационную безопасность для организации и контроля работы компьютерных и телекоммуникационных ресурсов и служб.

1.4. Ответственный за информационную безопасность вносит предложения директору ГАУ ДО РДОЦТ по назначению ответственных лиц из числа сотрудников для оперативного реагирования по устранению сбоев в работе компьютерных и телекоммуникационных ресурсов и служб, допуска к их обслуживанию, проведения поточных и плановых технических работ.

2. Порядок пользования вычислительной и оргтехникой и программным обеспечением

2.1. Сотрудник, пользующийся компьютерными и телекоммуникационными ресурсами и службами ГАУ ДО РДОЦТ (далее Пользователь) должен соблюдать правила техники безопасности, пожарной безопасности и инструкции о правилах работы с вычислительной и оргтехникой, программным обеспечением.

2.2. Каждый пользователь должен пройти инструктаж по безопасности труда на конкретном рабочем месте. Ответственность за соблюдение техники безопасности несет непосредственный руководитель пользователя.

2.3. Цель, методы и содержание работы с вычислительной и оргтехникой должны соответствовать должностным обязанностям пользователя.

2.4. Пользователям запрещается самостоятельно:

2.4.1. Отключать сетевое оборудование общего пользования.

2.4.2. Изменять конфигурацию, производить ремонт вычислительной и оргтехники.

2.4.3. Подключать периферийные устройства, не предусмотренные для конкретного рабочего места.

2.4.4. Отключать, разукомплектовывать и перемещать периферийные устройства и другое оборудование.

2.4.5. Устанавливать новое или модифицировать имеющееся системное, офисное, прикладное, сетевое и другие виды программного обеспечения. Необходимость замены (модификации, новой установки и т.п.) программного обеспечения определяется ответственными сотрудниками и проводится только ними.

2.4.6. Допускать к работе компьютерных и телекоммуникационных ресурсов и служб посторонних лиц.

2.4.7. Производить загрузку операционных систем со съемных носителей.

2.5. Пользователь должен уверенно знать операционную систему Windows и уметь пользоваться ее стандартным программным обеспечением, пакетом MS Office, всеми распространенными интернет-обозревателями, а так же тем ПО, которое необходимо для исполнения функциональных обязанностей.

2.6. Пользователь должен знать и уметь пользоваться тем антивирусным программным обеспечением, которое находится на его компьютере. Перед проведением любых операций с внешним носителем информации пользователь обязан произвести антивирусную проверку внешнего носителя информации. При отсутствии антивирусного программного обеспечения или его неработоспособности пользоваться компьютером запрещается.

В случае невозможности излечения внешнего носителя информации от вируса пользователь ставит об этом в известность ответственного за информационную безопасность, который производит соответствующие данной ситуации действия.

Пользователю категорически запрещается производить какие-либо действия с информацией зараженного вирусом внешнего носителя.

3. Основы защиты информации

3.1. Пользователь должен знать и уметь сохранять необходимую информацию либо на сменных носителях, либо на сервере.

Чаще всего информацию защищают от:

- физической утраты;
- удаления, изменения, порчи в результате использования нелицензионного программного обеспечения;
- порчи, изменения, удаления компьютерными вирусами и подобными им программами;
- несанкционированного доступа, изменения, просмотра, копирования и удаления посторонними лицами.

Физическая утрата информации может произойти из-за:

- выхода из строя носителя информации;
- кражи компьютера или носителя информации;
- стихийного бедствия;
- нарушения правил эксплуатации вычислительной техники и носителей информации.

Меры по предотвращению физической утраты информации:

- резервное копирование ценной информации;
- хранение и установка вычислительной техники и носителей информации в охраняемых и защищенных от внешних воздействий помещениях.

.

4. Ответственность за нарушение требований Инструкции

Данная инструкция обязательна для выполнения всеми сотрудниками ГАУ ДО РДОЦТ, имеющим доступ к компьютерным и телекоммуникационным ресурсам и службам ГАУ ДО

РДОЦТ. Руководитель структурного подразделения обязан ознакомить каждого работника подразделения с настоящей инструкцией под роспись.

За неисполнение или ненадлежащее исполнение настоящей Инструкции сотрудники ГАУ ДО РДОЦТ несут дисциплинарную ответственность в соответствии с действующим законодательством РФ.

5. Контроль за исполнением Инструкции

Контроль за исполнением настоящей Инструкции возлагается на ответственного за информационную безопасность сотрудника, уполномоченного приказом директора ГАУ ДО РДОЦТ, а также на руководителей структурных подразделений ГАУ ДО РДОЦТ.