СОГЛАСОВАНО
Председатель профкома
_____ /_____/
протокол № ____ от «___» _____202__г.

СОГЛАСОВАНО
Специалист по охране труда
_____ /_____/
«___» _____202__г.

УТВЕРЖДЕНО
Директор _____
_____
_____ /_____/
Приказ № ____ от "___"_____202__г.

Егорова Дарья Александровна

Подписан: Егорова Дарья Александровна
DN: C=RU, S=Краснодарский край, T=Директор, O="МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ "" СТАНЦИЯ ЮНЫХ ТЕХНИКОВ"", СНИЛС=13845218165, ИНН=340960448770, E=mboudodsutprim.aht@mail.ru, G=Дарья Александровна, SN=Егорова, CN=Егорова Дарья Александровна
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: место подписания
Дата: 2025-07-29 15:29:47
Foxit Reader Версия: 9.7.0

ИНСТРУКЦИЯ №14
по информационной безопасности

1. Общие положения.

2. Основная цель обеспечения информационной безопасности - предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в компьютерных системах учреждения.

3. Работники учреждения обязаны:

-Знать и соблюдать требования настоящей Инструкции и других документов по информационной безопасности при работе с ПК, имеющими доступ к информационным ресурсам локальной сети учреждения и сети «Интернет»;

-Знать и уметь правильно использовать то аппаратно - программное обеспечение, которое установлено на его ПК, а также строго выполнять правила работы со средствами защиты информации, установленными на них;

-Хранить в тайне свой пароль (пароли);

4. Выполнять следующие требования по антивирусному контролю:

-Антивирусный контроль всех дисков и файлов ПК должен проводиться ежедневно в начале работы при их загрузке в автоматическом режиме;

-Обновление антивирусных баз должно проводиться в соответствии с периодичностью, указанной в руководствах по применению конкретных антивирусных средств;

-В процессе работы обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (flesh-дисках, CD-, DVD- и т.п.). Разархивирование и контроль входящей информации должен проводиться непосредственно после ее приема. Контроль исходящей информации должен проводиться непосредственно перед архивированием и отправкой (записью на съемный носитель);

-Устанавливаемое (изменяемое) на ПК программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения на ПК лицом, установившим (изменившим) программное обеспечение, в присутствии пользователя ПК должна быть выполнена антивирусная проверка;

-При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник учреждения должен провести внеочередной антивирусный контроль своего ПК;

5. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов работники обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов инженера по защите информации, владельца зараженных файлов;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, немедленно приостановить работу и сообщить о данном факте директору учреждения;
- по факту обнаружения зараженных вирусом файлов составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия. Присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним ПК.

6. Работникам учреждения категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ПК в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПК или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами ПК;
-осуществлять обработку конфиденциальной информации (персональных данных) в присутствии посторонних (не допущенных к данной информации) лиц;
- осуществлять обработку конфиденциальной информации (персональных данных) при подключенном ПК к сети Интернет;
- записывать и хранить конфиденциальную информацию (персональные данные) на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенными без присмотра свои ПК, не активировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры), если таковые имеются;
- оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие конфиденциальную информацию;

- предпринимать попытки несанкционированного доступа к недоступным информационным ресурсам, осуществлять намеренное изменение, уничтожение, чтение, или передачу информации неавторизованным способом;

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок немедленно ставить в известность ответственного по защите информации.

7. Права работников, имеющих доступ к информационным ресурсам локальной сети и сети «Интернет».

7.1. Работники учреждения, пользователи ПК имеют право:

-Давать ответственному по защите информации предложения совершенствованию мер информационной безопасности в учреждении;

- Обращаться к ответственному по защите информации для оказания необходимой технической и методологической помощи в своей работе.

8. Ответственный по защите информации имеет право:

-Требовать от работников - пользователей ПК соблюдения установленных технологий обработки информации и выполнения инструкций и других документов по обеспечению безопасности и защите информации;

-Обращаться к руководителю с требованием прекращения работы сотрудников - пользователей ПК при несоблюдении ими установленных технологий обработки информации или невыполнении требований по обеспечению информационной безопасности;

-Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи информации и технических средств.

9. Ответственность.

Работники учреждения, пользователи ПК, имеющие доступ к информационным ресурсам локальной сети учреждения и сети «Интернет», несут персональную ответственность за обеспечение информационной безопасности при их использовании, и соблюдение требований настоящей Инструкции.