ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 199
ПРИМОРСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00EBFA1AC69E31BA2875EBCC8D26CD95A5
Владелец: Протасова Ольга Валерьевна
Действителен: с 26.06.2023 до 18.09.2024

УТВЕРЖДАЮ
Врио Директора
ГБОУ школа № 199
_____ Протасова О. В.
«18» июля 2023 г.

ИНСТРУКЦИЯ
пользователю по соблюдению режима защиты информации в ГБОУ школа №199 Приморского района

Санкт-Петербург, 2023

Настоящая Инструкция разработана для обеспечения защиты информации при использовании автоматизированных рабочих мест (АРМ) и телекоммуникационных ресурсов сотрудниками ГБОУ школа №199 (далее Школа). Все пользователи АРМ обязаны использовать компьютерные ресурсы квалифицированно, эффективно, придерживаясь правил этики и настоящей инструкции.

При несоблюдении пользователями условий настоящей инструкции к ним применяется административные меры взыскания, вплоть до увольнения, в соответствии со степенью вины, установленной служебным расследованием.

Организация не несет ответственность за действия отдельных пользователей, нарушивших настоящую инструкцию.

Организация имеет право, проверять любой или все аспекты компьютерной системы, в том числе электронную почту, с целью контроля соблюдения требований инструкции.

Средства информатизации предоставляются сотрудникам Школы для обеспечения эффективного выполнения их функциональных обязанностей.

При работе в локальной вычислительной сети (ЛВС) и АИСУ «Параграф» запрещается:

- Использовать компоненты программного и аппаратного обеспечения Школы в неслужебных целях;
- Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;
- Осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;
- Записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации (флешки и т.п.);
- Оставлять включенной без присмотра свою рабочую станцию, не активизировав средства защиты: выход из профиля;
- 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 - ставить в известность сотрудников ИТ отдела Школы и руководителя своего подразделения;

Системный администратор, руководители структурных подразделений и пользователи должны обеспечивать строгое соблюдение мер безопасности *с* целью защиты корпоративной сети от вирусов, поступающих по электронной почте. Для этого необходимо установить на каждом рабочем месте и почтовом сервере антивирусный пакет программ, позволяющих выявление наличия вирусов на самом раннем этапе.

Запрещается передача информации личного характера для решения личных проблем, а также информации по просьбе третьих лиц без согласования с руководством Школы.

Неверные, навязчивые, непристойные, клеветнические, оскорбительные, угрожающие или противозаконные материалы запрещается пересылать по электронной почте или с помощью других средств электронной связи, а также отображать и хранить на компьютерах. Пользователи, заметившие или получившие подобные материалы, должны сразу сообщить об этом инциденте своему руководителю.