УТВЕРЖДАЮ
Директор ГБОУ СОШ № 296
Фрунзенского района Санкт-Петербурга
_____ С.А.Алексеева
приказ № 98 от 25.06 2014 г.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

1. ОБЩИЕ ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ОБРАБОТКИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1. К защищаемой информации, обрабатываемой в информационных системах персональных данных ГБОУ СОШ № 296 Фрунзенского района Санкт-Петербурга (далее - ГБОУ СОШ № 296), относятся персональные данные, служебная (технологическая) информация системы защиты, другая информация конфиденциального характера в соответствии с "Перечнем защищаемых информационных ресурсов".

1.2. Действие настоящей Инструкции распространяется на ГБОУ СОШ № 296.

1.3. Обработка защищаемой информации в ГБОУ СОШ № 296 разрешается на основании приказа руководителя ГБОУ СОШ № 296.

1.4. Ответственность за организацию защиты информации в ГБОУ СОШ № 296 и выполнение установленных условий ее функционирования возлагается на администратора безопасности информации. Ответственность за выполнение мероприятий безопасности информации возлагается на лицо, производящее ее обработку (пользователя).

1.5. Допуск пользователей к работе в ГБОУ СОШ № 296 осуществляется в соответствии с "Перечнем лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей", утверждаемом руководителем ГБОУ СОШ № 296.

1.6. К самостоятельной работе на автоматизированных рабочих местах (АРМ), входящих в состав локальной сети ГБОУ СОШ № 296, допускаются лица, изучившие требования настоящей Инструкции и освоившие правила эксплуатации АРМ и технических средств защиты. Допуск производится после проверки знания настоящей Инструкции и практических навыков в работе.

1.7. Помещения, в которых размещены технические средства ГБОУ СОШ № 296, отвечают режимным требованиям и в нерабочее время закрываются в установленном порядке.

1.8. Вход в помещения, в которых производится автоматизированная обработка защищаемой информации, разрешается постоянно работающим в нем работникам, а также лицам, привлекаемым к проведению ремонтных, наладочных и других работ и посетителей в сопровождении работников ГБОУ СОШ № 296.

1.9. Техническое обслуживание и ремонт АРМ проводятся только уполномоченным лицом – инженером ЦИО ГБОУ СОШ № 296 . При проведении этих работ обработка защищаемой информации (ПДн) запрещается.

1.10. По фактам и попыткам несанкционированного доступа к защищаемой информации, а также в случаях ее утечки и (или) модификации (уничтожения) проводятся служебные расследования.

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

2.1. При первичном допуске к работе в ГБОУ СОШ № 296 пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных (регламентирующих) документов по вопросам безопасности при автоматизированной обработке информации, изучает настоящую Инструкцию, получает личный текущий пароль у должностного лица, выполняющего функции администратора безопасности информации в ГБОУ СОШ № 296 (далее - администратор безопасности).

2.2. Каждый работник ГБОУ СОШ № 296, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ГБОУ СОШ № 296, несет персональную ответственность[1] за свои действия и обязан:

2.2.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами.

2.2.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными в ГБОУ СОШ № 296.

2.2.3. Хранить в тайне свой пароль.

2.2.4. Передавать для хранения установленным порядком при необходимости свои реквизиты разграничения доступа только администратору безопасности ГБОУ СОШ № 296.

2.2.5. Выполнять требования по антивирусной защите в части, касающейся действий пользователей.

---

[1] Работники, виновные в нарушении режима защиты ПДн, несут дисциплинарную, гражданскую, административную, уголовную и иную предусмотренную законодательством Российской Федерации ответственность.

2.2.6. Немедленно ставить в известность администратора безопасности в следующих случаях:

- при подозрении компрометации личного пароля;

- обнаружения нарушения целостности пломб (наклеек) на аппаратных средствах АРМ или иных фактов совершения в отсутствие пользователя попыток несанкционированного доступа (НСД) к ресурсам ГБОУ СОШ № 296;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ГБОУ СОШ № 296;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию, выхода из строя или неустойчивого функционирования узлов или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

- некорректного функционирования установленных средств защиты;

- обнаружения непредусмотренных отводов кабелей и подключенных устройств;

- обнаружения фактов и попыток несанкционированного доступа и случаев нарушения установленного порядка обработки защищаемой информации.

2.3. Пользователю категорически запрещается:

2.3.1. Использовать компоненты программного и аппаратного обеспечения ГБОУ СОШ № 296 в неслужебных целях.

2.3.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ГБОУ СОШ № 296 или устанавливать дополнительно любые программные и аппаратные средства.

2.3.3. Осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц.

2.3.4. Записывать и хранить защищаемую информацию на неучтенных носителях информации (флеш-картах, DVD и CD-дисках, съемных дисках, картах памяти и т.п.).

2.3.5. Оставлять включенным без присмотра АРМ, не активизировав средства защиты от несанкционированного доступа.

2.3.6. Оставлять без личного присмотра на АРМ или где бы то ни было свои персональные реквизиты доступа, машинные носители и распечатки, содержащие защищаемую информацию.

2.3.7. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к ознакомлению с защищаемой информацией посторонних лиц. Об обнаружении такого рода ошибок ставить в известность администратора безопасности.

2.3.8. Производить перемещения технических средств АРМ без согласования с администратором безопасности.

2.3.9. Вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройств, производить техническое обслуживание

(ремонт) средств вычислительной техники без согласования с администратором безопасности и без оформления соответствующего Акта.

2.3.10. Подключать к АРМ нештатные устройства и самостоятельно вносить изменения в состав и конфигурацию.

2.3.11. Осуществлять ввод пароля в присутствии посторонних лиц.

2.3.12. Оставлять без контроля АРМ в процессе обработки конфиденциальной информации.

2.3.13. Привлекать посторонних лиц для производства ремонта (технического обслуживания) технических средств АРМ.