УТВЕРЖДАЮ
Директор школы
_____ Ю.Б. Ильина
31 августа 2020 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 1B91792F7F9F8CC2BEEACE3A16301B19B49210CF
Владелец: Ильина Юлия Борисовна
Действителен с 12.01.2021 по 12.04.2022

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
НАЧАЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 300
ЦЕНТРАЛЬНОГО РАЙОНА САНКТ-ПЕТЕРБУРГА

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 школы № 300 Центрального района Санкт-Петербурга, относятся персональные данные, служебная (технологическая) информация системы защиты, другая информация конфиденциального характера в соответствии с "Перечнем защищаемых информационных ресурсов ГБОУ школы № 300 Центрального района Санкт-Петербурга".

1.2. Действие настоящей Инструкции распространяется на ответственного за обработку персональных данных.

1.3. Обработка защищаемой информации в ГБОУ школе № 300 Центрального района Санкт-Петербурга разрешается на основании приказа руководителя.

1.4. Ответственность за организацию защиты информации в школе 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 школе осуществляется в соответствии с "Перечнем лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей", утверждаемом руководителем школы.

1.6. К самостоятельной работе на автоматизированных рабочих местах (АРМ) 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, отвечают режимным требованиям и в нерабочее время сдаются под охрану установленным порядком.

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 школы.

1.9. Техническое обслуживание АРМ, уборка помещения и т.п. проводятся только под контролем уполномоченного лица. 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 школе № 300 Центрального района Санкт-Петербурга 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 школе (далее - администратор безопасности).

2.2. Каждый работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным школы, 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 вшколе.

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.

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

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;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств;
- 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 НСД и случаев нарушения установленного порядка обработки защищаемой информации.

---

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

2.3. Пользователю категорически запрещается:

2.3.1. Использовать компоненты программного и аппаратного обеспечения в неслужебных целях.

2.3.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств 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 (гибких магнитных дисках и т.п.).

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

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.