Частное образовательное учреждение
дополнительного профессионального образования
«Промбезопасность»

«Утверждаю»

Директор ЧОУ ДПО «Промбезопасность»

_____С.М. Аленин

«_____» _____ 2017 г.

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных по обеспечению безопасности информации

г. Иваново
2017 год

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

К защищаемой информации, обрабатываемой в информационных системах персональных данных ЧОУ ДПО «Промбезопасность» (далее – Учебный центр), относятся персональные данные, служебная (технологическая) информация системы защиты, другая информация конфиденциального характера.

Обработка защищаемой информации в Учебном центре разрешается на основании приказа директора.

Ответственность за организацию защиты информации в Учебном центре и выполнение установленных условий ее функционирования возлагается на администратора безопасности информации.

Ответственность за выполнение мероприятий безопасности информации возлагается на лиц, производящих ее обработку (пользователей).

Допуск пользователей к работе осуществляется в соответствии с Перечнем лиц, допущенных к обработке персональных данных, утвержденным директором Учебного центра.

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.

Помещения, в которых размещены технические средства отвечают режимным требованиям.

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, посетителей в сопровождении работников Учебного центра.

Техническое обслуживание АРМ, уборка помещения и т.п. проводятся только под контролем уполномоченного лица Учебного центра. При проведении этих работ обработка защищаемой информации (ПДн) запрещается.

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

При первичном допуске к работе 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 (далее - администратор безопасности).

Каждый работник Учебного центра, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным, несет персональную ответственность <1> за свои действия и обязан:

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

Знать и строго выполнять правила работы со средствами защиты информации, установленными в Учебном центре.

Хранить в тайне свой пароль.

Передавать для хранения установленным порядком при необходимости свои реквизиты разграничения доступа только администратору безопасности Учебного центра.

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

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 Учебного центра;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств;
- отклонений в нормальной работе системных и прикладных программных средств, 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.

Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения в неслужебных целях.
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств или устанавливать дополнительно любые программные и аппаратные средства.
- осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц.
- записывать и хранить защищаемую информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.).
- оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД.

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

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

- 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.

- производить перемещения технических средств АРМ без согласования с администратором безопасности.

- 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 без оформления соответствующего Акта.

- подключать к АРМ нештатные устройства и самостоятельно вносить изменения в состав и конфигурацию.

- осуществлять ввод пароля в присутствии посторонних лиц.

- оставлять без контроля АРМ в процессе обработки конфиденциальной информации.

- привлекать посторонних лиц для производства ремонта (технического обслуживания) технических средств АРМ.