Приложение 6
к распоряжению Администрации
городского округа Химки
Московской области
от 30.09.2021 № 56-р

ПРОЕКТ ИНСТРУКЦИИ ПО ОБРАБОТКЕ ИНФОРМАЦИИ (ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ) СЕГМЕНТА ЕИСОУ

ИНСТРУКЦИЯ ПО ОБРАБОТКЕ ИНФОРМАЦИИ

(ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ)

СЕГМЕНТА ЕИСОУ

«УТВЕРЖДАЮ»

_____

(наименование должности, фамилия, инициалы)

_____

печать

«___»_____20__года

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет обязанности должностного лица (далее – пользователя), обрабатывающего информацию (в том числе персональных данных (далее – ПДн)), в Сегменте (далее – Сегмент) Единой информационной системы оказания государственных и муниципальных услуг Московской области (далее – Система) _____ (далее – Организация).

2 ОБЩИЕ ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ОБРАБОТКИ ИНФОРМАЦИИ В СИСТЕМЕ

2.1. К защищаемой информации, обрабатываемой в Системе, относятся ПДн, служебная (технологическая) информация системы защиты, другая информация конфиденциального характера в соответствии с «Перечнем защищаемых информационных ресурсов».

2.2. Обработка защищаемой информации в Сегменте разрешается на основании приказа руководителя Организации.

2.3. Ответственность за организацию защиты информации в Сегменте и выполнение установленных условий ее функционирования возлагается на администратора информационной безопасности информации Сегмента.

2.4. Ответственность за выполнение мероприятий безопасности информации возлагается на лицо, производящее ее обработку (пользователя Сегмента).

2.5. Допуск пользователей к работе в Сегменте осуществляется в соответствии с «Перечнем лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей», утверждаемом руководителем Организации.

2.6. К самостоятельной работе на автоматизированных рабочих местах (далее – АРМ), входящих в состав Сегмента, 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.

2.7. Помещения, в которых размещены технические средства Сегмента, отвечают режимным требованиям и в нерабочее время должны сдаваться под охрану установленным порядком.

2.8. Вход в помещения, в которых производится автоматизированная обработка защищаемой информации, разрешается постоянно работающим в них работникам, а также лицам, привлекаемым к проведению ремонтных, наладочных и других работ, и посетителей в сопровождении работников Организации.

2.9. Техническое обслуживание АРМ, уборка помещения и т.п. проводятся только под контролем уполномоченного лица Организации. При проведении этих работ обработка защищаемой информации запрещается.

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

3 ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

3.1. При первичном допуске к работе в Сегменте пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных (регламентирующих) документов в сфере информационной безопасности при автоматизированной обработке информации, изучает настоящую Инструкцию, получает личный текущий пароль у должностного лица, выполняющего функции администратора информационной безопасности в Организации (далее – администратор ИБ).

3.2. Работник Организации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным Сегмента, несет персональную ответственность за свои действия и обязан:

3.2.1. Неукоснительно соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами Сегмента.

3.2.2. Знать и неукоснительно выполнять правила работы со средствами защиты информации, установленными в Сегменте.

3.2.3. Хранить в тайне свой пароль.

3.2.4. Передавать для хранения в установленном порядке при необходимости сведения о своей учетной записи исключительно администратору ИБ Системы.

3.2.5. Выполнять требования правил антивирусной защиты в части, касающейся действий пользователей.

3.2.6. Немедленно ставить в известность администратора ИБ в следующих случаях:

– при подозрении компрометации личного пароля;

– при обнаружении нарушения целостности пломб (наклеек) на аппаратных средствах АРМ или иных фактов совершения в отсутствие пользователя попыток несанкционированного доступа (далее – НСД) к ресурсам Сегмента;

– при несанкционированных (произведенных с нарушением установленного порядка) изменениях в конфигурации программных или аппаратных средств Сегмента;

– при обнаружении отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию Сегмента, 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.

3.3. Пользователю категорически запрещается:

3.3.1. Использовать компоненты программного и аппаратного обеспечения Сегмента в неслужебных целях.

3.3.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств Сегмента или устанавливать дополнительно любые программные и аппаратные средства.

3.3.3. Записывать и хранить защищаемую информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.).

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

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

3.3.6. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к ознакомлению с защищаемой информацией посторонних лиц.

3.3.7. Производить перемещения технических средств АРМ без согласования с администратором ИБ.

3.3.8. Вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройств, производить техническое обслуживание (ремонт) средств вычислительной техники без согласования с администратором ИБ и без оформления соответствующего Акта. Подключать к АРМ нештатные устройства и самостоятельно вносить изменения в состав и конфигурацию.

3.3.9. Осуществлять ввод пароля в присутствии посторонних лиц, если есть риск его компрометации.

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

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

4 ОТВЕТСТВЕННОСТЬ

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

Начальник подразделения ИБ (подпись) И. О. Фамилия

СОГЛАСОВАНО:

Управление кадров (подпись) И. О. Фамилия

Юридический отдел (подпись) И. О. Фамилия

С инструкцией ознакомлен:

_____(подпись) _____ (расшифровка подписи)

«____» _____20___г.

_____(подпись) _____ (расшифровка подписи)

«____» _____20___г.

_____(подпись) _____ (расшифровка подписи)

«____» _____20___г.

_____(подпись) _____ (расшифровка подписи)

«____» _____20___г.

_____(подпись) _____ (расшифровка подписи)

«____» _____20___г.

_____(подпись) _____ (расшифровка подписи)

«____» _____20___г.