ИНСТРУКЦИЯ
пользователя информационной системы персональных данных

Настоящая Инструкция устанавливает порядок предоставления доступа к ПДн в информационной системе персональных данных (далее - ИСПДн) и обязанности пользователя ИСПДн по обеспечению безопасности обрабатываемых в ней ПДн, запреты на действия пользователя в ИСПДн, а также права пользователя ИСПДн.

1. Порядок предоставления доступа к информационной системе персональных данных

1.1. Работник ООО «Первый ГКЗ» наделяется правом доступа к ПДн в ИСПДн в соответствии с занимаемой должностью, должностной инструкцией и/или на основании приказа директора ООО «Первый ГКЗ».

1.2. Лицо, ответственное за допуск работников к ИСПДн обеспечивает организацию учета лиц, допущенных к работе с ПДн, прав и паролей доступа.

1.3. Контроль за выполнением настоящей Инструкции возлагается на администратора информационной безопасности ИСПДн.

1.4.

2. Обязанности пользователя ИСПДн

Пользователь обязан:

2.1. Не реже 1 раза в год посещать раздел “Работа с персональными данными” на сайте ООО «Первый ГКЗ» (www.firstgkz.ru) для актуализации знаний в сфере обработки и защиты ПДн.

2.2. Знать и соблюдать требования федерального закона “О персональных данных” и локальных актов ООО «Первый ГКЗ» в сфере обработки и защиты ПДн.

2.3. Исключить возможность неконтролируемого пребывания посторонних лиц в помещениях, где ведутся работы с ПДн.

2.4. Руководствоваться требованиями организационно-распорядительных документов ИСПДн. Строго соблюдать установленные правила обеспечения безопасности персональных данных при работе с программными и техническими средствами ИСПДн.

2.5. Использовать ИСПДн для выполнения служебных задач в соответствии с должностной инструкцией.

2.6. Использовать для доступа к ИСПДн собственную уникальную учетную запись (логин) и пароль.

2.7. Не допускать при работе с ИСПДн просмотр посторонними лицами персональных данных, отображаемых на дисплее автоматизированного рабочего места (далее - АРМ) или иных носителях.

2.8. Блокировать экран дисплея АРМ парольной заставкой при оставлении рабочего места.

2.9. По всем вопросам, связанным с обеспечением защиты персональных данных, содержащихся в базах данных, и работе со средствами защиты информации, возникающими при работе в ИСПДн, обращаться к администратору информационной безопасности.

2.10. Немедленно прекращать обработку персональных данных и ставить в известность администратора информационной безопасности при подозрении компрометации пароля, а также при обнаружении:

- несанкционированных изменений в конфигурации программных или аппаратных средств АРМ;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого

функционирования АРМ;

- непредусмотренных конфигурацией АРМ отводов кабелей и подключенных устройств;
- сообщений от программного обеспечения антивирусной защиты о возможном вирусном заражении АРМ или возникновении неисправностей (сбоев) в работе сервисов и информационных ресурсов ПГНИУ.
- других попыток несанкционированного доступа к ИСПДн.
-

3. Действия, запрещенные пользователю ИСПДн

Пользователю ИСПДн запрещается:

3.1. Предоставлять доступ к информации, содержащей ПДн, лицам, не допущенным к их обработке. Обрабатывать ПДн в присутствии лиц, не допущенных к их обработке.

3.2. Осуществлять ввод ПДн под диктовку.

3.3. Сообщать (или передавать) посторонним лицам личные ключи или атрибуты доступа к ресурсам ИСПДн.

3.4. Копировать информацию, содержащую ПДн на узлы сети, не входящие в ИСПДн.

3.5. Выводить на печать информацию, содержащую ПДн на принтеры, печать на которых не согласована с администратором информационной безопасности.

3.6. Осуществлять доступ к ИСПДн с узлов сети, не назначенных администратором информационной безопасности в качестве АРМ ИСПДн.

3.7. Самостоятельно изменять конфигурацию аппаратно-программных средств ИСПДн.

3.8. Осуществлять действия по преодолению установленных ограничений на доступ к ИСПДн.

3.9. Устанавливать на АРМ программное обеспечение, не связанное с исполнением служебных обязанностей.

3.10. Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с администратором информационной безопасности ИСПДн.

3.11.

4. Права пользователя ИСПДн

Пользователь ИСПДн имеет право:

4.1. Получать помощь по вопросам эксплуатации ИСПДн от администратора информационной безопасности.

4.2. Обращаться к администратору информационной безопасности по вопросам дооснащения АРМ техническими и программными средствами, не входящими в штатную конфигурацию АРМ и ИСПДн, необходимыми для автоматизации деятельности в соответствии с возложенными на него должностными обязанностями.

5. Правила работы в информационно-телекоммуникационных сетях международного информационного обмена

5.1. Работа в информационно-телекоммуникационных сетях международного информационного обмена - сети Интернет и других (далее - Сеть) на элементах ИСПДн должна проводиться только при служебной необходимости.

5.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирусных, межсетевых экранов и других);

- передавать по Сети защищаемую информацию;
- скачивать из Сети программное обеспечение и другие файлы в неслужебных целях;
- посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение, сайты знакомств, онлайн игры и другие).