Приложение 9

к приказу от 9 января 2023 г. №01/23-ПД

УТВЕРЖДАЮ
Генеральный директор
ООО "СК "УЛЫБНИСЬ"
_____ / Калачиков Н.В.
9 января 2023 г.

ИНСТРУКЦИЯ
По обеспечению безопасности персональных данных

1.Основные положения

1.1 Настоящий документ определяет основные обязанности, права и ответственность сотрудников ООО "СК "УЛЫБНИСЬ" при обработке персональных данных (далее – ПДн).

2. Общие требования

2.1 Каждый сотрудник, осуществляющий обработку ПДн, несет персональную ответственность за свои действия и обязан:

2.1.1 строго соблюдать требования данной Инструкции;

2.1.2 хранить в тайне личные пароли доступа;

2.1.3 обеспечивать сохранность внешних машинных носителей персональных данных;

2.1.4 соблюдать требования нормативных и локальных правовых актов, регламентирующих правила обеспечения безопасности и обработки ПДн;

2.1.5 помещать бумажные носители ПДн по завершении работы с ними на место хранения либо возвращать лицу, выдавшему их для работы;

2.1.6 немедленно информировать Ответственного за организацию обработки персональных данных:

- о факте утраты удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), печатей для опечатывания;
- о факте склонения к разглашению ПДн;
- о факте утери бумажных носителей персональных данных;
- о случаях или попытках несанкционированного проникновения в помещения, где осуществляется обработка ПДн;
- утери машинных носителей ПДн;
- подозрении на компрометацию личного пароля;
- при подозрении на совершение попыток несанкционированного доступа к ресурсам ИСПДн;
- при обнаружении несанкционированных изменений в конфигурации программного и аппаратного обеспечения ИСПДн;
- сбоев в работе системного или прикладного программного обеспечения, средств защиты информации;
- некорректного функционирования установленных средств защиты информации;
- обнаружения недокументированных свойств или ошибок системного и прикладного программного обеспечения;
- осуществлять хранение бумажных носителей ПДн только в местах, утвержденных Перечнем мест хранения материальных носителей персональных данных;

2.1.7 хранить бумажные носители персональных данных таким образом, чтобы исключить возможность просмотра персональных данных третьими лицами и лицами, не допущенными к обработке персональных данных данной категории в соответствие с перечнем должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (далее - неуполномоченные лица);

2.1.8 вносить уточнения в ПДн, содержащихся на бумажных носителях ПДн, посредством вычеркивания или вымарывания ПДн с применением пасты-штрих. Если внесение уточнений не позволяют особенности носителя ПДн, то этот носитель уничтожается и заменяется на новый;

2.1.9 Для хранения рабочих файлов в электронном виде использовать файловый сервер и(или) общую папку отдела.

2.2 Сотруднику запрещается:

2.2.1 использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;

2.2.2 хранить и обрабатывать личную информацию на АРМ и серверах ИСПДн.

2.2.3 использовать информационные ресурсы сети Интернет, содержание которых нарушает действующее законодательство Российской Федерации;

2.2.4 использовать информационные ресурсы сети Интернет для целей, не связанных со служебной деятельностью;

2.2.5 препятствовать работе средств защиты информации и средств резервного копирования информации;

2.2.6 самовольно вносить какие-либо изменения в конфигурацию программного и аппаратного обеспечения ИСПДн или устанавливать дополнительно любые программные и аппаратные средства;

2.2.7 использовать в работе неучтенные машинные носители ПДн;

2.2.8 умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты информации;

2.2.9 бесконтрольно оставлять носители ПДн или передавать их на хранение другим лицам;

2.2.10 выносить носители персональных данных (в том числе бумажные документы) за пределы помещений, если это не связано с выполнением должностных обязанностей сотрудника

2.2.11 оставлять одних в помещении лиц, не имеющих права самостоятельного доступа в помещения (в том числе при проведении работ по уборке и техническом обслуживании оборудования);

2.2.12 разглашать ПДн в беседах с посторонними лицами, а также с сотрудниками, если этого не требуется для исполнения им своих служебных обязанностей;

2.2.13 передавать ПДн по незащищенным каналам связи (в том числе, с использованием общедоступных почтовых серверов типа mail.ru, yandex.ru и прочих);

2.2.14 размещать и хранить ПДн на ресурсах, не предусмотренных технологическим процессом обработки ПДн в ИСПДн;

2.2.15 использовать поступающие из сторонних организаций внешние машинные носители информации без предварительной проверки их на наличие вирусов. При обнаружении на носителе зараженного и не поддающегося лечению файла дальнейшее использование носителя не допускается;

2.2.16 обрабатывать ПДн в случае сбоев в работе средств защиты информации;

2.2.17 самовольно вносить изменения в поля типовых форм документов.

3. Обязанности сотрудника при осуществлении антивирусной защиты

3.1 При возникновении подозрения о наличии вредоносного ПО (появления на экране монитора неожиданных сообщений или изображений, баннеров, самопроизвольного запуска программ, появления сообщения-предупреждения от брандмауэра или антивируса, что некое приложение (программа) пытается соединиться с интернетом, хотя эту программу не запускали) Сотрудник самостоятельно может провести внеочередной антивирусный контроль своего АРМ, либо обратиться Ответственному за обеспечение безопасности ПДн.

3.2 В случае отсутствия возможности запустить антивирусную проверку (заблокирован доступ к ОС, антивирус не запускается/ отсутствует), при наличии деструктивного воздействия вируса на файлы, лечение которых антивирусной программой невозможно, а также в случае сбоя обновления антивирусных баз, либо в случае сбоя при проведении антивирусного сканирования сотрудник должен сообщить об этом Ответственному за обеспечение безопасности ПДн.

3.3 Сотрудник обязан:

- в случае, если антивирусная программа не работает в фоновом режиме, самостоятельно проводить проверку антивирусной программой всех файлов, полученных из Интернет, посредством электронной почты, а также копируемых на АРМ или ресурс ИС с любых внешних машинных носителей информации;
- контролировать результат и успешность выполнения антивирусной проверки;
- сообщить о факте заражения вирусами Ответственному за обеспечение безопасности ПДн.

3.4 Сотруднику запрещается:

- предпринимать попытки отключения установленных на АРМ антивирусных программ и их удаления;
- производить настройки (конфигурирование) антивирусных программ;
- препятствовать проведению полной антивирусной проверки, запускаемой по расписанию, по возможности, не вести в данное время никакие работы на АРМ;
- самостоятельно устанавливать на АРМ любые антивирусные средства;
- использовать ресурсы Интернет (осуществлять обмен сообщениями электронной почты) в случае сбоев в работе средств антивирусной защиты;
- самостоятельно производить устранение последствий от воздействия вредоносных программ;
- каким-либо образом влиять на работу антивирусных программ.

4. Обязанности сотрудника при осуществлении парольной защиты

4.1 При получении одноразового пароля, сотрудник должен авторизоваться в операционной системе и произвести смену одноразового пароля на постоянный личный пароль. Постоянный личный пароль должен соответствовать следующим требованиям Положения по организации парольной политики.

4.2 При получении постоянного пароля сотрудник обязан хранить его в индивидуальном сейфе или опечатанном шкафу, или запомнить пароль и уничтожить путем измельчения конверта с паролем.

4.3 В случае компрометации личного пароля (когда пароль стал или может быть известен еще кому-либо кроме владельца данного пароля, невозможности входа при правильном вводе личного пароля, изменение расположения иконок программ и файлов на рабочем столе, несанкционированного изменения файлов, хранящихся в ИСПДн) владелец скомпрометированного пароля должен немедленно сообщить о факте утери или компрометации пароля Ответственному за обеспечение безопасности ПДн. В случае компрометации обязательно производится смена пароля.

4.4 При оставлении рабочего места сотрудник должен завершить открытую сессию в прикладном программном обеспечении и операционной системе, либо использовать функцию «блокировка экрана» операционной системы.

4.5 Сотруднику запрещается:

- передавать кому-либо личный пароль;

- хранить в общедоступном месте пароли доступа;
- записывать личный пароль доступа на бумажный носитель в открытом виде;
- осуществлять ввод пароля в присутствии лиц, которые потенциально могут увидеть процесс набора пароля;
- использовать чужие идентификаторы и пароли доступа;
- оставлять без присмотра включенное АРМ, не осуществив блокировку экрана.
- Сотрудник несет ответственность за сохранность своего личного пароля и за действия, совершенные в ИСПДн под выданной ему учетной записью.

5. Защита ПДн от утечки по видовым каналам

5.1 При возникновении угрозы просмотра ПДн неуполномоченными лицами, необходимо прекратить обработку ПДн, а бумажные носители разместить таким образом, чтобы был исключен просмотр ПДн (перевернуть текстом вниз, убрать в ящик стола или хранилище).

5.2 Осуществлять работу с документами, содержащими персональные данные, только при исключении возможности их просмотра через окна (закрытие штор, жалюзи, монитор отвернут от окна).

6. Ответственность за неисполнение (ненадлежащее исполнение) настоящей инструкции

6.1 Все сотрудники несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией в соответствии с внутренними локальными актами и действующим законодательством Российской Федерации.