

УТВЕРЖДАЮ



Директор МАУ ДО ЦС «Вымпел»

Г.О. г. Кумертау РБ

Р.И.Хайретдинов

" _____ 2023 г.

**Инструкция пользователя
В Муниципальном автономном учреждении
дополнительного образования Центр спорта «Вымпел»
городского округа город Кумертау Республики Башкортостан**

РАЗРАБОТАЛ

Администратор информационной
безопасности

_____ А. Ибрагимов И.Р.
подпись _____ расшифровка

подписи

" _____ " _____ 2023 г.

Г.Кумертау
2023 год

1. Общие положения

1.1. Инструкция устанавливает обязанности пользователя *МАУ ДО ЦС «Вымпел» ГО г.Кумертау РБ* по обеспечению безопасности обрабатываемых в организации персональных данных, запреты на действия пользователя, а также его права и ответственность (далее соответственно – инструкция, ИСПДн, организация).

1.2. Доступ пользователя к ИСПДн осуществляется в соответствии с перечнем сотрудников, допущенных к обработке персональных данных.

1.3. Привилегии доступа пользователя к автоматизированному рабочему месту (далее – АРМ) назначаются в соответствии с матрицей прав доступа.

1.4. Контроль за исполнением требований, изложенных в инструкции, возлагается на сотрудника, ответственного за обеспечение безопасности персональных данных.

1.5. Каждый сотрудник организации, участвующий в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным, в части компетенции, в дальнейшем именуемый пользователь, несет персональную ответственность за свои действия при работе с информационными ресурсами.

2. Обязанности пользователя

2.1. Пользователь обязан:

при работе с документами, содержащими персональные данные, руководствоваться требованиями организационно-распорядительных документов;

строго соблюдать установленные правила обеспечения безопасности персональных данных при работе с программными и техническими средствами;

использовать ИСПДн для выполнения служебных задач в соответствии с должностной инструкцией;

использовать для доступа к ИСПДн собственную уникальную учетную запись (логин) и пароль;

хранить в тайне пароли и PIN-коды, обеспечивать физическую сохранность ключевого носителя доступа к ИСПДн;

не допускать при работе с ИСПДн просмотр посторонними лицами персональных данных, отображаемых на дисплее АРМ;

блокировать экран дисплея АРМ парольной заставкой при оставлении рабочего места;

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

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

нарушений целостности пломб, наклеек на ПЭВМ (персональные электронно-вычислительные машины), при наличии таковых, или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД);

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.

2.3. Немедленно информировать ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн в случае обнаружения попыток несанкционированного доступа к ИСПДн.

2.4. Немедленно информировать сотрудников, осуществляющих сетевое администрирование организации, при появлении сообщений от программного обеспечения антивирусной защиты о возможном вирусном заражении АРМ или возникновении неисправностей (сбоев) в работе сервисов и информационных ресурсов организации.

3. Действия, запрещенные пользователю

3.1. Пользователю запрещается:

- предоставлять доступ к информации, содержащей персональные данные, лицам, не допущенным к их обработке;
- записывать пароль на любые носители, в том числе бумажные;
- сообщать (или передавать) посторонним лицам личные ключи или атрибуты доступа к ресурсам;
- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных;
- работать с персональными данными в присутствии посторонних (не допущенных к данной информации) лиц;
- самостоятельно изменять конфигурацию аппаратно-программных средств;
- осуществлять действия по преодолению установленных ограничений на доступ;
- отключать или изменять конфигурацию средств защиты информации.
- устанавливать на АРМ программное обеспечение, не связанное с исполнением должностных обязанностей.

4. Права пользователя

4.1. Пользователь имеет право:

- получать помощь по вопросам эксплуатации систем от ответственного за систему защиты информации;
- обращаться к сотрудникам, осуществляющим сетевое администрирование организации, по вопросам дооснащения АРМ техническими и программными средствами, не входящими в штатную конфигурацию АРМ, необходимыми для автоматизации деятельности в соответствии с возложенными на него должностными обязанностями;
- подавать сотрудникам, осуществляющим сетевое администрирование организации, предложения по совершенствованию функционирования ИСПДн.

5. Ответственность пользователя

5.1. Пользователь несет ответственность за:

- обеспечение безопасности персональных данных при их обработке;
- нарушение работоспособности или вывод из строя системы защиты;
- преднамеренные действия, повлекшие модификацию или уничтожение персональных данных, и несанкционированный доступ к персональным данным;
- разглашение персональных данных.

5.2. Пользователь, имеющий расширенные права «Опытный пользователь» или «Администратор», несет ответственность за корректное функционирование прикладного программного обеспечения ИСПДн.

5.3. За нарушение настоящей инструкции к пользователю могут применяться меры дисциплинарного воздействия.

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

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

6.2. При работе в сети запрещается:

осуществлять работу при отключенных средствах защиты (антивирусных и других);
передавать по сети защищаемую информацию без использования средств шифрования;
скачивать из сети программное обеспечение и другие файлы в неслужебных целях;
посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение (ПО), сайты знакомств, онлайн игры и другие).

7. Перечень локальных нормативных актов, ознакомление с которыми рекомендуется в целях соблюдения требований настоящей инструкции

Инструкция пользователя на случай возникновения внештатных ситуаций.

Инструкция администратора информационной безопасности.

Разрешительная система доступа к персональным данным, содержащимся в базах данных ИСПДн.

Инструкция по использованию паролей.

Инструкция по архивации информационных ресурсов системы.

Инструкция по антивирусной безопасности.

[illegible]