Приложение 3
к приказу от 01.09.2023 №114-о

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ ГБПОУ РО «ЗТАТ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

Пользователем информационных систем персональных данных (далее – Пользователь) является уполномоченный сотрудник ГБПОУ РО «ЗТАТ» (далее – Учреждение).

Пользователь должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности персональных данных (далее – ПД).

В своей деятельности, связанной с обработкой ПД, Пользователь руководствуется Политикой в отношении обработки персональных данных в ГБПОУ РО «ЗТАТ» и настоящей Инструкцией.

Пользователи, участвующие в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющие доступ к аппаратным средствам, программному обеспечению и обрабатываемой информации, несут персональную ответственность за свои действия.

2. ОБЯЗАННОСТИ И ПРАВА ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Пользователь обязан:

- соблюдать требования Политики в отношении обработки персональных данных в ГБПОУ РО «НКПТИУ» и иных локальных актов Учреждения, устанавливающих порядок работы с ПД;

- выполнять в информационных системах персональных данных (далее – ИСПД) только те процедуры, которые необходимы для исполнения его должностных обязанностей;

- использовать для выполнения должностных обязанностей только предоставленное ему автоматизированное рабочее место (далее – АРМ) на базе персонального компьютера;

- пользоваться только зарегистрированными в установленном порядке съемными (отчуждаемыми) машинными носителями информации;

- обеспечивать безопасное хранение вышеуказанных материальных носителей информации, исключающее несанкционированный доступ к ним;

- немедленно сообщать руководителю структурного подразделения или ответственному за обеспечение безопасности ПД в ИСПД (далее – Ответственный) о нештатных ситуациях, фактах и попытках несанкционированного доступа к обрабатываемой информации, о блокировании, исчезновении (искажении) защищаемой информации;

- перед началом обработки в ИСПД файлов, хранящихся на съемных носителях информации, осуществлять проверку файлов на наличие компьютерных вирусов. Антивирусный контроль на АРМ должен осуществляться Пользователем не реже одного раза в неделю;

- располагать экран монитора в помещении во время работы так, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами;

- соблюдать установленный режим разграничения доступа к информационным ресурсам;

- получать пароль, надежно его запоминать и хранить в тайне.

Пользователям ИСПД запрещается:

- записывать и хранить информацию, относящуюся к конфиденциальной информации или ПД, на неучтенных материальных носителях информации;

- оставлять во время работы материальные носители информации без присмотра, несанкционированно передавать материальные носители информации другим лицам и выносить их за пределы помещения, в котором производится обработка информации;

- отключать средства антивирусной защиты; отключать (блокировать) средства защиты информации;

- производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

- самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

- обрабатывать в ИСПД информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам ИСПД;

- сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам в ИСПД;

- работать в ИСПД при обнаружении каких-либо неисправностей;

- хранить на учтенных носителях информации программы и данные, не относящиеся к рабочей информации;

- вводить в ИСПД ПД под диктовку или с микрофона;

- привлекать посторонних лиц для производства ремонта технических средств ИСПД без согласования с Ответственным.

Пользователь имеет право знакомиться с внутренними документами Учреждения, регламентирующими его обязанности по занимаемой должности.

3. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ ПРИ РАБОТЕ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ

Пароли доступа к ИСПД устанавливаются Ответственным или Пользователем.

При формировании пароля необходимо руководствоваться следующими требованиями:

- длина пароля должна быть не менее 8-и символов;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АРМ, общепринятые сокращения) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации;

- запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

- запрещается использовать ранее использованные пароли.

При организации парольной защиты запрещается:

- записывать свои пароли в очевидных местах, таких как внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

- хранить пароли в записанном виде на отдельных листах бумаги;

- сообщать свои пароли посторонним лицам, а также сведения о применяемых средствах защиты от несанкционированного доступа.

4. ПОРЯДОК ПРИМЕНЕНИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

Плановую смену паролей на доступ в ИСПД рекомендуется проводить один раз в месяц.

Пользователь обязан незамедлительно сообщить Ответственному факты утраты, компрометации ключевой, парольной и аутентифицирующей информации.

Внеплановая смена личного пароля должна производиться в обязательном порядке в следующих случаях:

- компрометации (подозрении на компрометацию) пароля;

- прекращения полномочий (увольнение, переход на другую работу внутри организации) Пользователя (в течение 24 часов после окончания последнего сеанса работы данного Пользователя с ИСПД);

- по инициативе Ответственного.

5. ТЕХНОЛОГИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

При первичном допуске к работе с ИСПД Пользователь:

- проходит инструктаж по использованию ИСПД;

- знакомится с требованиями действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПД;

- получает у Ответственного идентификатор и личный пароль для входа в ИСПД.

Перед началом работы Пользователь визуально проверяет целостность пломб, убеждается в отсутствии посторонних технических средств, включает необходимые средства вычислительной техники.

Авторизацию в ИСПД (ввод личного идентификатора и пароля) Пользователь осуществляет при отсутствии в помещении посторонних лиц.

В процессе работы на АРМ ИСПД Пользователь использует технические средства и установленное Ответственным программное обеспечение согласно Техническому паспорту ИСПД.

Копирование ПД на электронные носители информации осуществляется только при наличии производственной необходимости и только на учтенные электронные носители информации.

При необходимости создания на АРМ Пользователя дополнительных электронных документов, содержащих ПД, Пользователь создает и хранит такие документы в строго отведенном для этого месте.

Печать документов, содержащих ПД, осуществляется только при наличии производственной необходимости на принтер, подключенный Ответственным к АРМ Пользователя. Все бумажные носители, не подлежащие учету по каким-либо техническим или иным причинам (сбой принтера при печати, обнаружение ошибок в документе после распечатки и т.д.) уничтожаются незамедлительно. Распечатанные черновые бумажные варианты вновь создаваемых документов, содержащих ПД, уничтожаются незамедлительно после подписания (утверждения) окончательного варианта документа.

В случае возникновения необходимости временно покинуть рабочее помещение во время работы в ИСПД, Пользователь обязан выключить компьютер либо заблокировать его. Разблокирование компьютера производится набором пароля разблокировки, который был создан при настройке системы блокировки АРМ. При отсутствии в покидаемом помещении других сотрудников Учреждения, Пользователь обязан закрыть дверь помещения на ключ или другой используемый ограничитель доступа.

Покидая рабочее помещение в конце рабочего дня, Пользователь обязан выключить все необходимые средства вычислительной техники и закрыть дверь помещения на ключ.