Частное образовательное учреждение высшего образования
«Международный Институт Дизайна и Сервиса»
(ЧОУВО МИДиС)

УТВЕРЖДЕНО
приказом Ректора
от 26.05.2025 № 10-01-02/179

_____М.В. Усынин

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Пл-8.5.3-МИДиС-26
Дата введения 26 мая 2025 г.

Челябинск 2025

Инструкция пользователя информационных систем персональных данных рассмотрена и рекомендована к внедрению решением ученого совета ЧОУВО МИДиС протокол № 10 от 26.05.2025.

Разработчики:

Проректор учебно-проектной работе Н.А. Попова

23.05.2025
(дата)

Начальник отдела ОТОиСИТ Д.С. Татьянин

23.05.2025
(дата)

1. Общие положения

1.1. Инструкция пользователя информационных систем персональных данных (далее – Инструкция) определяет порядок обеспечения информационной безопасности при проведении работ пользователями информационных систем персональных данных (далее – ИСПДн) ЧОУВО МИДиС (далее – Организация).
1.2. Настоящая Инструкция разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
1.3. Пользователи получают свои права на доступ к ресурсам ИСПДн через администратора безопасности информационных системах персональных данных (далее – АБ).

2. Термины и определения

2.1. Автоматизированное рабочее место – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.
2.2. Доступ к информации – возможность получения информации и ее использования.
2.3. Защита информации – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.
2.4. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
2.5. Информация – сведения (сообщения, данные) независимо от формы их представления.
2.6. Несанкционированный доступ – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.
2.7. Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.
2.8. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
2.9. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).
2.10. Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

3. Обязанности пользователя информационных систем персональных данных

Пользователь обязан:

3.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации.
3.2. Выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры, которые определены технологическим процессом обработки информации.
3.3. Знать и соблюдать установленные требования к обработке персональных данных, учету и хранению носителей информации, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.
3.4. Соблюдать требования парольной политики.
3.5. Получить уникальное имя и персональный идентификатор (при его наличии) от АБ. Пользователь обязан помнить и соблюдать в тайне свои имена и пароли, не допускается их запись на каких-либо носителях в целях напоминания.
3.6. Во время работы располагать экран монитора так, чтобы затруднить посетителям просмотр отображаемой информации. Жалюзи или шторы на окнах должны быть закрыты.
3.7. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) совместно с АБ провести внеочередной антивирусный контроль своего АРМ.
3.8. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения:

- приостановить обработку данных;
- немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения АБ, владельца зараженных файлов;
- произвести лечение или уничтожение зараженных файлов (для выполнения требований данного пункта привлечь АБ).

3.9. Немедленно вызывать АБ и поставить в известность руководителя структурного подразделения при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа к защищаемой АРМ;
- несанкционированных (произведенных с нарушением установленного порядка) 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 узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на АРМ технических средств защиты;
- непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

3.10. При утере или подозрении на утечку своего имени, пароля и персональных идентификаторов пользователь должен немедленно сообщить об этом АБ.

3.11. Обо всех выявленных нарушениях, связанных с информационной безопасностью Организации, а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться к АБ.
3.12. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <⊞><L>.
3.13. В ИСПДн осуществляется блокирование сеанса доступа пользователя после 10 минут его бездействия (неактивности) в информационной системе.
3.14. Принимать меры по реагированию в случае возникновения внештатных и аварийных ситуаций с целью ликвидации их последствий в пределах, возложенных на него функций.
3.15. Пользователям запрещается:

- разглашать защищаемую информацию посторонним лицам;
- копировать защищаемую информацию на неучтенные внешние носители;
- самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный порядок функционирования технических и программных средств;
- подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- выполнять на АРМ работы, не предусмотренные технологическим процессом обработки персональных данных;
- сообщать (или передавать) посторонним лицам параметры своей учетной записи (имя, персональный идентификатор (при его наличии) и пароль) в ИСПДн;
- оставлять без присмотра и передавать другим лицам персональный идентификатор;
- привлекать посторонних лиц для ремонта или настройки АРМ без согласования с ответственным за обеспечение безопасности персональных данных;
- оставлять без присмотра свое АРМ, не активизировав блокировку доступа, или оставлять свое АРМ включенным по окончании работы;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

4. Порядок работы пользователя с ресурсами информационных систем персональных данных

4.1. Начало работы на ПЭВМ
При включении ПЭВМ необходимо дождаться завершения загрузки и готовности системы защиты информации и операционной системы к идентификации пользователя.
Идентификация пользователя осуществляется по уникальному имени и паролю с использованием персонального идентификатора, если таковой предусмотрен системой защиты информации. Для получения доступа к ресурсам ИСПДн пользователь должен приложить к считывателю персональный идентификатор (при его наличии) и ввести с клавиатуры свой пароль.
Если после ввода пароля средство защиты информации выдаст сообщение об ошибке идентификации пользователя, пользователь должен обратиться к АБ.
4.2. Завершение работы на ПЭВМ

По окончании работы пользователь должен либо завершить штатными средствами сеанс своей работы (без выключения ПЭВМ), либо завершить работу ПЭВМ стандартным способом (при этом выключить ПЭВМ).

4.3. Требования к распечатыванию информации

Все распечатываемые документы должны быть учтены. Бракованные бумажные носители и черновики документов должны быть уничтожены.

4.4. При отсутствии пользователя на рабочем месте либо в присутствии лиц, не имеющих допуска к ресурсам ИСПДн, все документы, содержащие персональные данные, должны быть недоступны для просмотра и иного их использования.

5. Организация парольной защиты

5.1. Личные пароли доступа к элементам ИСПДн создаются самостоятельно.

5.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 6 месяцев.

5.3. Правила формирования пароля:

- пароль должен состоять не менее чем из 6 символов;
- в пароле должны присутствовать символы из числа прописных и строчных букв английского алфавита от A до Z; десятичных цифр (от 0 до 9); символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);
- запрещается использовать в качестве пароля имя учетной записи, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения пользователей ИСПДн и их родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно вычислить, основываясь на информации о пользователе;
- 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.);
- запрещается выбирать пароли, которые уже использовались ранее.

5.4. Правила ввода пароля:

- ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами.

5.5. Правила хранения пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям личный пароль и/или регистрировать их в системе под своей учетной записью.

5.6. Пользователи обязаны:

- четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;
- своевременно сообщать АБ об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

6. Ответственность

6.1. Пользователь несет персональную ответственность за:

- сохранность носителей информации и содержащейся на них информации (в рабочее время);
- соблюдение требований данной Инструкции, неправомерное использование ресурсов ИСПДн и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

6.2. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн работники могут быть привлечены к ответственности, предусмотренной действующим законодательством Российской Федерации.

Согласовано

Начальник юридического отдела

_____ А.А. Аполовников

26.05.2025

(дата)