



УТВЕРЖДАЮ

Директор ЛОГКУ «Леноблэкомиллиция»

А.В. Слюньков

«02» декабря 2024 г.

ИНСТРУКЦИЯ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДн)

Настоящая инструкция определяет действия пользователей ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн. Обработка информации и ПДн в ИСПДн осуществляется в рамках технологических процессов. Пользователи должны выполнять свои функциональные обязанности в соответствии с утвержденными регламентами данных процессов. При сборе информации и ПДн работники должны руководствоваться принципом достоверности и достаточности информации и ПДн для установленных регламентами технологических процессов целей обработки, а также недопустимости обработки персональных данных, избыточных по отношению к заявленным целям. Состав собираемых и обрабатываемых ПДн утвержден в рамках каждого процесса. С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в ИСПДн в учреждении назначается приказом администратор безопасности; с целью контроля выполнения необходимых мероприятий по обеспечению безопасности ответственный за защиту информации. Допуск пользователей для работы в ИСПДн осуществляется на основании Заявки на регистрацию. В заявке указывается:

1. Должность (с полным наименованием подразделения), фамилия, имя и отчество работника, контактные данные работника (телефон, кабинет).
2. Основание для регистрации учетной записи (номер приказа о принятии на работу в учреждение или иного договорного документа. Заявку подписывает руководитель учреждения, подтверждающий, что указанный работник действительно принят в штат учреждения. Заявка согласуется с администратором и передается в отдел информационной безопасности министерства.

Процедура предоставления (или изменения) прав доступа пользователя к ресурсам ИСПДн определена заявкой. Если в ходе исполнения должностных обязанностей при работе в ИСПДн необходимо лишить пользователя

полномочий или необходимо добавить пользователю полномочия по доступу к ресурсам ИСПДн, то необходимо предоставить администратору безопасности заявку о блокировке. При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение работника) учетная запись должна немедленно блокироваться. Руководитель с момента увольнения сотрудника, должен в 3-х дневный срок направить заявку на блокирование учетной записи в администратору информационной безопасности учреждения.

Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. Для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в Журнале учета машинных носителей.

Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (далее - СВТ), входа в систему и все действия при работе в ИСПДн. Вход пользователя в систему может осуществляться только под своей учетной записью и по персональному паролю.

При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на средствах вычислительной техники. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями Инструкции по антивирусной защите.

Каждый пользователь, участвующий в рамках своих функциональных обязанностей в работе в ИСПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн. Соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с ПДн при ее обработке;
- незамедлительно сообщать администратору информационной безопасности и в отдел информационной безопасности министерства об инцидентах информационной безопасности при работе с ИСПДн;
- незамедлительно сообщать в отдел информационных технологий министерства о плановых/внеплановых перебоях в системе электроснабжения;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на средствах вычислительной техники, с помощью которой производится работа в ИСПДн;
- хранить в тайне свой пароль (пароли) в соответствии с Инструкцией по парольной защите;

- хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу). При выходе в течение рабочего дня из служебной комнаты (помещения) убирать документы с конфиденциальной информацией (ПДн) и съемные цифровые носители в сейф (металлический шкаф) и запирать их на ключ;
- выполнять требования Правил антивирусной защиты в ИСПДн в полном объеме;
- немедленно известить ответственного за защиту информации и отдел информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении: несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения; некорректного функционирования установленных на компьютеры технических средств защиты;
- непредусмотренных отводов кабелей и подключенных устройств. Пользователю категорически запрещается: использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратнопрограммных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;
- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц при работе с ИСПДн; записывать и хранить конфиденциальную информацию из ИСПДн (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;
- подключение к структурированной кабельной сети аппаратных средств минуя средства защиты информации, в том числе криптографические;
- размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, а именно экраны видеомониторов в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами.