Инструкция пользователя
при работе в ИСПДн в
ГБОУ РК «Ливадийская санаторная школа-интернат»

2020

1. **Общие положения**

1.1. Настоящая инструкция разработана на основании:
- Федерального закона Российской Федерации от 27.07.2006 г. №152-ФЗ «О персональных данных»;
- Положения «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства Российской Федерации № 781 от 17 ноября 2007 г.;
- Постановлением от 1 ноября 2012 г. № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных ситемах персональных данных”;

1.2. Данная инструкция определяет общие обязанности, права и ответственность пользователя информационной системы персональных данных (далее – ИСПДн) ГБОУ РК «ЛСШИ» (далее - ЛСШИ) по обеспечению информационной безопасности при работе с ПДн.

1.3. Пользователем ИСПДн (далее – Пользователь) является сотрудник ЛСШИ, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн.

1.4. Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими нормативными, организационно- распорядительными документами по вопросам информационной безопасности.

1.5. Положения инструкции обязательны для исполнения всеми пользователями и доводятся под роспись. Пользователь должен быть предупрежден о возможной ответственности за ее нарушение.

2. Обязанности пользователя

2.1. При выполнении работ в ИСПДн Пользователь обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами в ИСПДн, правила работы и порядок регистрации в ИСПДн, доступа к информационным ресурсам ИСПДн;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (АРМ);
- хранить в тайне свои идентификационные данные (имена, пароли и т.д.);
- выполнять требования «Инструкции по парольной защите в информационной системе персональных данных», предъявляемые к парольной системе (нормативы на длину, состав, периодичность смены пароля и т.д.), осуществлять вход в ИСПДн только под своими идентификационными данными;
- передавать для хранения установленным порядком свое индивидуальное

устройство идентификации, личную ключевой носитель и другие реквизиты разграничения доступа, только руководителю своего подразделения или администратору безопасности ИСПДн (ответственному за информационную безопасность подразделения);

- выполнять требования «Инструкции по организации антивирусной защиты» в части, касающейся действий пользователей ИСПДн;

- выполнять требования «Инструкции по работе с корпоративной почной»;

- знать и выполнять требования положения о положение о порядке обработки и обеспечении безопасности ИСПД;

- немедленно вызывать администратора безопасности ИСПДн (ответственного за безопасность информации) и ставить в известность руководителя подразделения в случае утери персональной ключевых носителей, индивидуального устройства идентификации или при подозрении о компрометации личных ключей, паролей, данных, а также при обнаружении нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к зачищенной АРМ, несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ, некорректного функционирования установленных на АРМ технических средств защиты, непредусмотренных отводов кабелей и подключенных устройств;

- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним АРМ ставить в известность администратора безопасности ИСПДн (ответственного за безопасность информации) при необходимости внесения изменения в состав аппаратных и программных средств АРМ;

- работать в ИСПДн только в разрешенный период времени;

- немедленно выполнять предписания администраторов безопасности ИСПДн, предоставлять свое АРМ администратору безопасности для контроля;

- ставить в известность администраторов ИСПДн в случае появления сведений или подозрений о фактах НСД к информации, своей или чужой, а также 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;

- осуществлять установленным порядком уничтожение информации, содержащей сведения конфиденциального характера, с машинных носителей информации и из оперативной памяти АРМ;

- уважать права других пользователей на конфиденциальность и право пользования общими ресурсами;

- сообщать руководителю своего подразделения обо всех проблемах, связанных с эксплуатацией ИСПДн.

2.2. Пользователю категорически **ЗАПРЕЩАЕТСЯ:**

- использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;
- самовольно вносить какие-либо изменения в состав, размещение, конфигурацию аппаратно-программных средств ИСПДн (в том числе АРМ) или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формуляром АРМ;
- осуществлять обработку информации, содержащей сведения конфиденциального характера, в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.), в том числе для временного хранения;
- оставлять включенное без присмотра свое АРМ, не активизировав временную блокировку экрана и клавиатуры (средствами защиты от НСД или операционных систем);
- передавать кому-либо свое индивидуальное устройство идентификации (персональный ключевой носитель) в нарушение установленного порядка, делать неучтенные копии ключевого носителя, и вносить какие-либо изменения в файлы ключевого устройства идентификации;
- оставлять без личного присмотра на рабочем месте или где бы то ни было свою персональный ключевой носитель, персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения конфиденциального характера);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках ИСПДн (в том числе средств защиты), которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность администратора безопасности ИСПДн (ответственного за безопасность информации) и руководителя своего подразделения;
- подбирать и отгадывать чужие пароли, а также собирать информацию о других пользователях;
- осуществлять попытки НСД к ресурсам системы и других пользователей, проводить рассылку ложных, беспокоящих или угрожающих сообщений;
- фиксировать свои учетные данные (пароли, имена, идентификаторы, ключи) на материальных и нематериальных носителях;
- разглашать ставшую известной в ходе выполнения своих обязанностей информацию, содержащую сведения конфиденциального характера;
- вносить изменения в файлы, принадлежащие другим пользователям.

3. Права пользователя

3.1. Пользователь имеет право:

- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним АРМ;

- участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИСПДн, если данное нарушение произошло под его идентификационными данными;

- своевременно получать доступ к информационным ресурсам ИСПДн, необходимым ему для выполнения своих должностных обязанностей;

- требовать от администратора безопасности смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

4. Ответственность пользователя

4.1. Пользователь несет персональную ответственность за:

- ненадлежащее исполнение своих функциональных обязанностей, а также сохранность комплекта АРМ, съемных носителей информации, и целостность установленного программного обеспечения.

- разглашение сведений, отнесенных к сведениям конфиденциального характера, и сведений ограниченного распространения, ставших известными ему по роду работы;

- нарушение функционирования ИСПДн, уничтожение, блокирование, копирование, фальсификацию информации несет пользователь, под чьими идентификационными данными было совершено нарушение. Мера ответственности устанавливается по итогам служебного расследования.

4.2. Пользователи, виновные в нарушениях несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно-распорядительными документами «ЛСШИ».