Государственное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа №113
с углубленным изучением информационно-технологического профиля
Приморского района Санкт-Петербурга

Утверждаю

Директор

_____ Е.А. Касавцова

приказ от 28.01.2014 №74

Инструкция
по обеспечению безопасности персональных данных, обрабатываемых в информационной системе персональных данных

1. Общие положения

1.1. Настоящая Инструкция устанавливает обязанности пользователя информационных систем персональных данных (далее - ИСПДн) в ГБОУ школе №113 Приморского района Санкт-Петербурга (далее – образовательное учреждение) по обеспечению безопасности обрабатываемых в них персональных данных, запреты на действия пользователя в ИСПДн, а также его права и ответственность.

1.2. Доступ пользователя к ИСПДн осуществляется в соответствии с перечнями с перечнем сотрудников, допущенных к обработке персональных данных и перечнем сотрудников, допущенных к работе с персональными данными.

1.3. Привилегии доступа пользователя к АРМ назначаются в соответствии с матрицей прав доступа для ИСПДн.

1.4. Контроль за выполнением настоящей Инструкции возлагается на ответственного за обеспечение безопасности персональных данных.

2. Обязанности пользователя ИСПДн

Пользователь обязан:

2.1. Использовать ИСПДн для выполнения служебных задач в соответствии с должностной инструкцией.

2.2. Использовать для доступа к ИСПДн собственную уникальную учетную запись (логин) и пароль.

2.3. Хранить в тайне пароли и PIN-коды, обеспечивать физическую сохранность ключевого носителя доступа к ИСПДн.

2.4. Не допускать при работе с ИСПДн просмотр посторонними лицами персональных данных, отображаемых на дисплее АРМ.

2.5. Блокировать экран дисплея АРМ парольной заставкой при оставлении рабочего места.

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

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

3. Действия, запрещенные пользователю ИСПДн

Пользователю ИСПДн запрещается:

3.1. Предоставлять доступ к информации, содержащей персональные данные, лицам, не допущенным к их обработке.

3.2. Самостоятельно изменять конфигурацию аппаратно-программных средств ИСПДн.

2.4. Типовые формы документов должны быть составлены таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.
2.5. Хранение документов, содержащих персональные данные, осуществляется в металлических шкафах или сейфах.
2.6. Уничтожение документов, содержащих персональные данные, осуществляется способом, не позволяющим в дальнейшем ознакомиться с персональными данными.

3. Обязанности сотрудника, допущенного к обработке персональных данных
3.1. При работе с документами, содержащими персональные данные, сотрудник обязан исключить возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними (в том числе другими работниками школы).
3.2. При выносе документов, содержащих персональные данные, за пределы территории образовательного учреждения по служебной необходимости сотрудник должен принять все возможные меры, исключающие утрату (утерю, хищение) таких документов.
3.3. При утрате (утере, хищении) документов, содержащих персональные данные, работник обязан немедленно доложить о таком факте специалисту по кадрам, ответственному за систему защиты информации в информационной системе персональных данных, директору образовательного учреждения. По каждому такому факту назначается служебное расследование.

4. Сотрудникам, допущенным к обработке персональных данных запрещается:
4.1. Сообщать сведения, являющиеся персональными данными, лицам, не имеющим права доступа к этим сведениям.
4.2. Делать неучтенные копии документов, содержащих персональные данные.
4.3. Оставлять документы, содержащие персональные данные, на рабочих столах без присмотра.
4.4. Покидать помещение, не поместив документы с персональными данными в закрываемые сейфы, шкафы.
4.5. Выносить документы, содержащие персональные данные, из помещений школы без служебной необходимости.

5. Ответственность
5.1. Ответственность за неисполнение или ненадлежащее выполнение требований настоящей Инструкции возлагается на работников и руководителей подразделений.
5.2. Контроль за выполнением положений настоящей Инструкции возлагается на специалиста по кадрам, ответственного за систему защиты информации в информационной системе персональных данных.
5.3. За нарушение правил обработки персональных данных, их неправомерное разглашение или распространение, виновные лица несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.
5.4. В случае если в результате действий работника был причинен подлежащий возмещению работодателем ущерб третьим лицам, работник несет перед работодателем материальную ответственность в соответствии с главой 39 Трудового кодекса РФ.
5.5. В случае разглашения персональных данных, ставших известными работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника, трудовой договор с работником может быть расторгнут работодателем (подпункт «в» пункта 6 статьи 81 Трудового кодекса РФ).