Муниципальное бюджетное учреждение дополнительного образования «Детская музыкальная школа с. Тастуба муниципального района Дуванский район республики Башкортостан»

РАССМОТРЕНА
протокол общего собрания
работников ОУ
от «28» ноябр 2019г.
№ 9

УТВЕРЖДЕНА
приказ директора
Е.В.Ахметгалеевой
от «28» ноябр 2019 г.
№ 43/2

ИНСТРУКЦИЯ
Пользователя информационных систем персональных данных

1. Общие положения

1.1. Инструкция пользователя информационных систем персональных данных (далее – ИСПДн) (далее – Инструкция) определяет функциональные обязанности, права и ответственность пользователей информационных систем персональных данных (ИСПДн) , в которых обрабатываются персональные данные (далее – ПДн).

1.2. Настоящая Инструкция подготовлена в соответствии с требованиями нормативно-методических документов ФСТЭК России и ФСБ России по защите персональных данных, обрабатываемых с использованием средств автоматизации.

1.3. В настоящей Инструкции используются следующие понятия и определения:

1. автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;
2. база данных – объективная форма представления и организации совокупности данных, систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ;
3. информация – сведения (сообщения, данные) независимо от формы их представления;
4. персональные данные – любая информация, относящаяся к прямо или косвенно определённому, или определяемому физическому лицу (субъекту персональных данных);
5. информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
6. компрометация пароля – утрата доверия к тому, что используемый пароль обеспечивает безопасность персональных данных. К событиям, приводящим к компрометации пароля, относятся следующие события (включая, но не ограничиваясь): несанкционированное сообщение пароля другому лицу; утеря бумажного или машинного носителя информации, на котором был записан пароль; запись пароля на бумажном, машинном, ином носителе информации, доступ к которому не контролируется;
7. конфиденциальность персональных данных – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

8. несанкционированный доступ к персональным данным – доступ к персональным данным с нарушением установленных прав доступа, приводящий к нарушению конфиденциальности персональных данных, к утечке, искажению, подделке, уничтожению, блокированию доступа к персональным данным;
9. 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;
10. распространение персональных данных – действия, направленные на раскрытие персональных данных определённому лицу или неопределённому кругу лиц;
11. разглашение персональных данных – распространение персональных данных без согласия субъекта персональных данных или наличия иного законного основания;
12. средство защиты информации (СЗИ) – программные, программно-аппаратные, аппаратные средства, предназначенные и используемые для защиты персональных данных в ИС «Сетевой город. Образование»;
13. утеря пароля – события, приводящие к невозможности восстановления пароля в памяти лица, владеющего данным паролем;
14. электронная вычислительная машина ИСПДн (ЭВМ) – персональный компьютер, предназначенный для автоматизации деятельности пользователей и входящий в состав ИСПДн. В состав ЭВМ входят: системный блок, монитор, клавиатура, мышь, внешние устройства (локальный принтер, сканер и т.д.), программное обеспечение.

2. Обязанности пользователя

2.1. Пользователь информационных систем персональных данных (далее – ИСПДн) обязан:

2.1.1. Хранить в тайне ПДн, ставшие ему известными во время работы или иным путём и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки ПДн немедленно информировать Ответственного за организацию обработки персональных данных, Администратора информационных систем персональных данных (далее – ИСПДн) или Администратора ИБ.

2.1.2. При определении ПДн, подлежащих защите, использовать «Перечень персональных данных, обрабатываемых в «ДМШ с. Тастуба».

2.1.3. Знать и выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах в соответствии с Инструкциями, требованиями, регламентирующими функционирование установленных средств защиты.

2.1.4. Хранить в тайне свой пароль доступа в ИСПДн а также информацию о системе защиты, установленной ИСПДн.

2.1.5. Использовать для работы, только учтённые съёмные накопители информации (гибкие магнитные диски, компакт-диски и т.д.).

2.1.6. Сообщать о необходимости обновления антивирусных баз, случаях обнаружения или подозрениях о наличии вредоносного программного обеспечения, а также обо всех случаях нештатного функционирования средства антивирусной защиты Администратору ИСПДн.

2.1.7. Немедленно ставить в известность Администратора информационных систем персональных данных и (или) Администратора информационных систем персональных данных:

1. в случае утери носителя с конфиденциальной информацией (персональными данными) и (или) при подозрении компрометации личных ключей и паролей;
2. нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа к информационной системе персональных данных.
3. несанкционированных (произведённых с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств информационных систем персональных данных.

2.1.8. В случае 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 в информационных систем персональных данных технических средств защиты ставить в известность Администратора информационных систем персональных данных и (или) Администратора ИСПДн.

2.1.9. В случае увольнения пользователь ИСПДн обязан вернуть все документы и материалы, относящиеся к ИСПДн . В том числе: отчёты, инструкции, служебную переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к ИСПДн полученные в течение срока работы.

2.1.10. Уборка помещений должна производиться под контролем пользователя ИСПДн имеющего доступ в помещение и постоянно в нем работающего.

2.1.11. Вынос технических средств ИСПДн, на которой проводилась обработка персональных данных, за пределы контролируемой зоны с целью их ремонта, замены и т.п. без согласования с Администратором ИСПДн или Ответственным за организацию обработку ПДн запрещён. При принятии решения о выносе компьютеров, жёсткие магнитные диски должны быть демонтированы. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.

2.1.12. АРМ, используемые для работы с персональными данными, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора лицами, не допущенными к работе с обрабатываемыми на АРМ персональными данными.

2.2. Пользователю категорически запрещается:

1. передавать, устно или письменно, или иным способом ПДн лицам, не допущенным к работе с этими ПДн;
2. использовать ПДн при подготовке открытых публикаций, докладов, научных работ и т.д.;
3. выполнять работы с документами, содержащими ПДн, на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения Ответственного за организацию обработки персональных данных;

4. оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие ПДн, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами, содержащими ПДн;
5. использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;
6. самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать дополнительно любые программные и аппаратные средства;
7. осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;
8. записывать и хранить ПДн на неучтённых носителях информации (гибких магнитных дисках и т.п.);
9. оставлять включённой без присмотра своё АРМ, не активизировав средства защиты информации от НСД (временную блокировку экрана и клавиатуры);
10. умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность Администратора ИСПДн.

2.3. Принимать меры по реагированию, в случае возникновения нештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах, возложенных на него функций.

2.4. Оперативно докладывать Администратору ИСПДн о случаях возникновения нештатных ситуаций и аварийных ситуаций.

2.5. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов ИСПДн».

2.6. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

3. Права пользователя

3.1. Пользователь имеет право:

1. требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей;
2. получать доступ к информации, материалам, техническим средствам, помещениям, необходимых для надлежащего исполнения своих обязанностей.

4. Ответственность пользователя

4.1. Пользователь несёт ответственность за соблюдение требований настоящей инструкции, а также нормативных документов в области защиты информации.

4.2. За разглашение ПДн, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

4.3. Пользователи, виновные в несоблюдении настоящей инструкции расцениваются как нарушители ФЗ РФ 27.07.2006 г. № 152-ФЗ «О персональных данных» и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.