УТВЕРЖДАЮ
Директор МАСУ
Тайгинского городского округа
«Спортивный комплекс «Юность»
_____ А.А. Бахтина
01.07.2022 г.

Инструкция
по организации резервирования и восстановления программного обеспечения, баз персональных данных информационной системы персональных данных МАСУ Тайгинского городского округа «Спортивный комплекс «Юность»

1. Настоящая инструкция разработана с целью обеспечения возможности незамедлительного восстановления персональных данных в информационной системе персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных МАСУ Тайгинского городского округа «Спортивный комплекс «Юность».

2. Резервированию подлежат базы данных и файлы, содержащие персональные данные.

3. Резервирование выполняется штатным средством архивирования системы и данных «ntbackup» и производится на локальный дисковый массив. Процедура резервного копирования производится каждый день.

4. Ответственный за процедуру резервирования и восстановления назначается ответственный за организацию обработки персональных данных.

5. Восстановление файлов производится путём разархивирования файлов базы данных в исходный каталог.

УТВЕРЖДАЮ
Директор МАСУ
Тайгинского городского округа
«Спортивный комплекс «Юность»
_____ А.А. Бахтина
01.07.2022 г.

Инструкция пользователя информационной системы персональных данных при возникновении нештатных ситуаций

1. Настоящая инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных систем персональных данных МАСУ Тайгинского городского округа «Спортивный комплекс «Юность» (далее – ИСПДн), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания работоспособности в случае реализации рассматриваемых угроз.

3. Задачами данной Инструкции являются:

- определение мер защиты от прерывания работоспособности;
- определение действий по восстановлению в случае прерывания работоспособности.

4. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн, имеющих доступ к ресурсам ИСПДн, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

5. Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении № 1.

6. При реагировании на инцидент важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

- Уровень 1. Незначительный инцидент – локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты;

- Уровень 2. Авария – любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты;

- Уровень 3. Катастрофа – любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, к уничтожению,

блокированию, неправомерной модификации или компрометации защищаемых персональных данных, а также к угрозе жизни пользователей ИСПДн.

7. При возникновении нештатной ситуации любого уровня пользователь обязан оповестить ответственного за организацию обработки персональных данных, сообщив характер аварийной ситуации, масштаб ситуации по предварительной субъективной оценке.

8. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за организацию обработки персональных данных в Журнале регистрации фактов нарушения и восстановления работоспособности оборудования или ИСПДн. В кратчайшие сроки, не превышающие одного рабочего дня, должны быть предприняты меры по восстановлению работоспособности ИСПДн.

9. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные (программно-аппаратные) и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Все критичные помещения, в которых размещаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации восстановления ИСПДн описан в Инструкции по организации резервирования и восстановления программного обеспечения, баз персональных данных ИСПДн.

10. Ответственный за организацию обработки персональных данных:

- ознакомляет всех сотрудников, находящихся в его зоне ответственности, с данной инструкцией в рок, не превышающий 3-х рабочих дней с момента выхода нового сотрудника на работу;
- обучает пользователей, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.

Пользователи ИСПДн должны получить базовые знания в следующих областях:

- оказание первой медицинской помощи;
- пожаротушение;
- эвакуация людей;
- защита материальных и информационных ресурсов;
- методы оперативной связи со службами спасения и руководителями структурных подразделений;
- выключение оборудования, электричества, водоснабжения, газоснабжения;
- по окончанию ознакомления сотрудников получает их роспись в Журнале учёта прохождения первичного инструктажа.

11. Навыки и знания пользователей ИСПДн по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение пользователей ИСПДн порядку действий при возникновении аварийной ситуации. Ответственность за организацию обучения пользователей ИСПДн несёт

ответственный за организацию обработки персональных данных. Директор МАСУ Тайгинского городского округа «Спортивный комплекс «Юность» согласует сроки и порядок их обучения.

Приложение 1
к Инструкции пользователя ИСПДн
при возникновении нештатной ситуации

Источники угроз безопасности персональных данных

Технологические угрозы:
- Пожар в здании;
- Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения);
- Взрыв (бытового газа, взрывчатых веществ или приборов, работающих под давлением);
- Химический выброс в атмосферу.

Внешние угрозы:
- Массовые беспорядки;
- Сбои общественного транспорта;
- Эпидемия;
- Массовое отравление персонала;
- теракт.

Стихийные бедствия:
- Удар молнии;
- Сильный снегопад;
- Сильные морозы;
- Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания;
- Затопление водой в период паводка;
- Наводнение, вызванное проливным дождём;
- Торнадо;
- Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод).

ИТ-угрозы:
- Сбой системы кондиционирования в серверном помещении;
- Выход из строя файлового сервера;
- Частичная потеря информации на сервере без потери его работоспособности;
- Выход из строя локальной сети;
- Выход из строя рабочей станции;
- Частичная потеря информации на рабочей станции без потери её работоспособности.

Угроза, связанная с человеческим фактором:
- Ошибка персонала, имеющего доступ к элементам ИСПДн;
- Нарушение конфиденциальности, целостности и доступности конфиденциальной информации, а также несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.

Угрозы, связанные с внешними поставщиками:
- Отключение электроэнергии;
- Сбой в работе Интернет-провайдера;
- Физический разрыв внешних каналов связи.

УТВЕРЖДАЮ
Директор МАСУ
Тайгинского городского округа
«Спортивный комплекс «Юность»
А.А. Бахтина
01.07.2022 г.

Инструкция пользователя информационной системы персональных данных МАСУ Тайгинского городского округа «Спортивный комплекс «Юность»

1. Пользователем информационной системы персональных данных МАСУ Тайгинского городского округа «Спортивный комплекс «Юность» (далее – Пользователь) является любой работник МАСУ Тайгинского городского округа «Спортивный комплекс «Юность», осуществляющий обработку персональных данных в информационной системе персональных данных МАСУ Тайгинского городского округа «Спортивный комплекс «Юность» (далее – ИСПДн).

Согласно ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» обработка ПДн – 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 (далее - ПДн).

2. Пользователь в своей работе руководствуется настоящей Инструкцией, Положением об обеспечении безопасности ПДн, руководящими и нормативными документами ФСТЭК и ФСБ России и внутренними нормативными актами МАСУ Тайгинского городского округа «Спортивный комплекс «Юность», с которыми он был ознакомлен при прохождении первичного инструктажа.

3. Пользователь несёт персональную ответственность за свои действия.

4. Пользователь обязан:

- знать и выполнять требования Положения об обработке данных, Политики в отношении обработки данных, других локальных актов оператора в отношении персональных данных;

- знать и выполнять установленные требования по режиму обработки ПДн, учёту, хранению и использованию носителей ПДн, обеспечению безопасности ПДн;

- соблюдать требования парольной политики;

- блокировать АРМ в случае отсутствия на рабочем месте;

- оповещать ответственного за обеспечение безопасности ПДн о фактах нарушения информационной безопасности и возникновения нештатных ситуаций;

- при возникновении нештатных и аварийных ситуаций действовать согласно Инструкции пользователя при возникновении нештатных ситуаций с целью ликвидации их последствий и возможного ущерба.

5. Пользователю запрещается:

- разглашать обрабатываемые ПДн;
- производить несанкционированное копирование ПДн на учтенные носители;
- производить копирование ПДн на неучтенные носители;
- оставлять незаблокированным АРМ при отсутствии на рабочем месте;
- сообщать и передавать третьим лицам личные пароли и атрибуты доступа к ресурсам ИСПДн.

6. За нарушение информационной безопасности Пользователь несёт ответственность согласно действующему законодательству Российской Федерации.

УТВЕРЖДАЮ
Директор МАСУ
Тайгинского городского округа
«Спортивный комплекс «Юность»
_____ А.А. Бахтина
01.07.2022 г.

Инструкция
по учёту лиц, допущенных к работе с персональными данными в информационных системах персональных данных МАСУ Тайгинского городского округа «Спортивный комплекс «Юность»

1. Настоящая инструкция определяет порядок учёта лиц, допущенных к работе с персональными данными в информационных системах персональных данных МАСУ Тайгинского городского округа «Спортивный комплекс «Юность» (далее – ИСПДн).

2. Порядок допуска работника к работе с персональными данными:

- утверждение приказом о допуске к обработке персональных данных перечня должностей работников, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей (далее – Перечень);

- прохождение первичного инструктажа, включающего ознакомление со всеми нормативными документами, регламентирующими работу с персональными данными, согласно Инструкции по проведению инструктажа лиц, допущенных к работе с персональными данными с внесением соответствующей информации в Журнал учёта прохождения первичного инструктажа сотрудниками, допущенными к работе с персональными данными в ИСПДн;

- внесение записи учёта прав доступа к ИСПДн.

3. Допуск работника к персональным данным прекращается:

- в случае обнаружения нарушений порядка обработки персональных данных до выяснения и устранения причин нарушений;

- в случае увольнения сотрудника с момента подписания приказа об увольнении;

- при изменении его служебных обязанностей с момента утверждения нового Перечня.

УТВЕРЖДАЮ
Директор МАСУ
Тайгинского городского округа
«Спортивный комплекс «Юность»
А.А. Бахтина
01.07.2022 г.

Инструкция
по учёту и хранению съёмных носителей персональных данных МАСУ Тайгинского городского округа «Спортивный комплекс «Юность»

1. Общие положения

1.1. Настоящая «Инструкция по учёту и хранению съёмных носителей персональных данных» (далее – Инструкция) определяет порядок работы со съёмными носителями персональных данных в МСУ Тайгинского городского округа «Спортивный комплекс «Юность» (далее – Оператор) в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными нормативными правовыми актами РФ в области защиты персональных данных.

1.2. С Инструкцией знакомятся под подпись и выполняют её все лица, допущенные к обработке персональных данных «Приказом р допуске к обработке персональных данных».

2. Определения

Съёмный носитель персональных данных – носитель информации, используемый для хранения и передачи персональных данных в электронной форме.

Пользователь – работник Оператора или сотрудник по договору гражданско-правового характера, допущенный к обработке персональных данных «Приказом о допуске к обработке персональных данных».

3. Порядок работы со съёмными носителями

3.1. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, выдаёт съёмные носители пользователям только в случаях производственной необходимости.

3.2. Все съёмные носители персональных данных учитываются и выдаются пользователям под подпись.

3.3. Пользователям, получившим съёмные носители персональных данных под подпись, запрещается передавать их третьим лицам.

3.4. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, изымает съёмные носители персональных данных при увольнении пользователя.

3.5. Все съёмные носители персональных данных хранятся в запираемых шкафах или сейфах (металлических шкафах) с кодовыми или внутренними замками (с не менее чем двумя дубликатами ключей).

3.6. Допускается хранение съёмных носителей персональных данных вне запираемых шкафов или сейфов (металлических шкафов) при условиях уничтожения персональных данных в соответствии с Инструкцией по порядку и обезличивания персональных данных, либо если на съёмном носителе персональных данных хранятся только персональные данные в зашифрованном или обезличенном виде.

3.7. Право на перемещение съёмных носителей информации за пределы территории, на которой осуществляется обработка, имеют только те лица, которым это необходимо для выполнения своих должностных обязанностей.

3.8. Использование неучтённых съёмных носителей для обработки персональных данных фиксируется как несанкционированное, а ответственный за обеспечение безопасности персональных данных инициирует служебную проверку. По факту выясненных обстоятельств составляется Акт проведения расследования инцидента.

3.9. Пользователи, в случаях утраты или кражи съёмных носителей персональных данных, сообщают об этом ответственному за обеспечение безопасности персональных данных.

3.10. Съёмные носители персональных данных, пришедшие в негодность, или отслужившие в установленный срок, подлежат уничтожению в соответствии с Инструкцией по порядку уничтожения и обезличивания персональных данных. По результатам уничтожения составляется акт уничтожения персональных данных.

4. Порядок организации учёта съёмных носителей

4.1. На каждом съёмном носителе персональных данных размещается этикетка с уникальным учётным номером.

4.2. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, при выдаче, приёме, уничтожении съёмных носителей персональных данных вносит в Журнал учёта съёмных носителей персональных данных (Приложение 1):

- учётный номер, размещённый на этикетке на съёмном носителе персональных данных;
- тип съёмного носителя (USB-накопитель, внешний жёсткий диск, CD/DVD диск);
- серийный или инвентарный номер съёмного носителя;
- место хранения (номер запираемого шкафа или сейфа, номер помещения);
- дату и номер Акта уничтожения персональных данных в случае уничтожения съёмного носителя;
- подпись.

4.3. Пользователи при получении либо сдаче съёмных носителей персональных данных заносят в Журнал учёта съёмных носителей персональных данных свои фамилию, имя, отчество, ставят дату и подпись.

5. Ответственность

5.1. Все работники Оператора, допущенные в установленном порядке к работе с персональными данными, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством за обеспечение сохранности и соблюдению правил работы с персональными данными.

5.2. Ответственность за доведение требований настоящей Инструкции до работников Оператора несёт ответственный за организацию обработки персональных данных.

5.3. Ответственность за обеспечение мероприятий по реализации требований настоящей Инструкции, в том числе учёт, выдачу, уничтожение съёмных носителей персональных данных несёт ответственный за обеспечение безопасности персональных данных.