Росгидромет
Федеральное государственное бюджетное учреждение
«ЗАПАДНО-СИБИРСКОЕ УПРАВЛЕНИЕ ПО ГИДРОМЕТЕОРОЛОГИИ И МОНИТОРИНГУ ОКРУЖАЮЩЕЙ СРЕДЫ»
(ФГБУ «Западно-Сибирское УГМС»)
20.11.2022 № 22-96

УТВЕРЖДАЮ
Начальник
_____ А. О. Люцигер
«20» 11 2022 г.
М.П.

Инструкция пользователя информационных систем персональных данных по обеспечению безопасности обработки персональных данных при возникновении нештатных ситуаций в ФГБУ "Западно-Сибирское УГМС"

1. Основные понятия, термины и сокращения

В настоящем документе используются следующие основные понятия, термины и сокращения:

Администратор информационной безопасности - администратор информационной безопасности при организации работы ИСПДн и технической защиты в них информационных ресурсов, содержащих ПДн.

ИТС - информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

ИСПДн - информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации.

ЛВС - локальная вычислительная сеть.

Неправомерные действия с ПДн – действия, повлекшие неправомерный доступ, уничтожение, модифицирование, блокирование, копирование, предоставление, распространение, а также иные действия в отношении ПДн.

Нештатная ситуация - некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн.

ПДн - персональные данные.

Пользователь ИСПДн - работник ФГБУ "Западно-Сибирское УГМС" участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и/или имеющий доступ к аппаратным средствам, программному обеспечению и средствам защиты.

ПО - программное обеспечение.

2. Назначение

Настоящая Инструкция определяет наиболее распространенные нештатные ситуации, связанные с работой информационных систем персональных данных (далее - ИСПДн), функционирующих в ФГБУ "Западно-Сибирское УГМС", а также меры, принимаемые для восстановления работоспособности ИСПДн после возникновений нештатных ситуаций.

Действие настоящей Инструкции распространяется на всех пользователей ИСПДн, а также на работников ФГБУ "Западно-Сибирское УГМС", ответственных за основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении нештатных ситуаций.

В случае возникновения нештатной ситуации, администратором информационной безопасности совместно с ответственным за организацию обработки персональных данных в ФГБУ "Западно-Сибирское УГМС" (далее – ответственные специалисты) разрабатывается конкретный план действий с учетом текущей ситуации.

3. Порядок реагирования на нештатную ситуацию

Нештатная ситуация становится возможной в результате реализации одной либо нескольких угроз, приведенных в Приложении № 1.

3.1 Действия при возникновении нештатной ситуации

Пользователь ИСПДн, обнаруживший сбой в функционировании элементов ИСПДн, немедленно сообщает об этом специалистам отдела ЗС РВЦ.

Начальник учреждения в первую очередь выясняет причины нештатной ситуации и предпринимает действия по ее устранению, при необходимости привлекает ответственных специалистов:

- В случае сбоя в системе жизнеобеспечение здания (электро-, тепло-, водоснабжение, водоотведение) Начальник учреждения подключает к работе специалистов (электрика, сантехника, рабочего), которые проверяют работоспособность соответствующего оборудования и устраняют поломку.

- В случае сбоя программного обеспечения, обнаружения потери, уничтожения, модифицирования, блокирования, копирования, потери данных, иных причин – ответственные специалисты выясняют причину и последствия сбоя. Проводят мероприятия по устранению последствий сбоя: антивирусную проверку, целостность и работоспособность ПО, целостность и работоспособность оборудования и другие. При необходимости производится восстановление ПО и данных из последней резервной копии. Если исправить ошибку своими силами не удалось, то ответственные специалисты обращаются за помощью к специалистам по разработке и внедрению ПО.

- В случае сбоя в ЛВС, ИТС, выхода из строя сервера ответственные специалисты поручают работникам, по функциональным обязанностям, отвечающим за работу соответствующего оборудования, определить и устранить возникшие в оборудовании проблемы.

- При обнаружении утечки информации (уязвимость в системе защиты) проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищенности системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.

- При попытке несанкционированного доступа проводится анализ ситуации, по результатам которого, в случае необходимости, принимаются меры по предотвращению попытки несанкционированного доступа, так же производится устранение выявленных недостатков. Рекомендуется провести внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует применить такие обновления.

- При компрометации ключей следует руководствоваться инструкциями к применяемой системе криптозащиты.

- При компрометации или подозрения на компрометацию пароля пользователь обязан незамедлительно произвести смену пароля.

- В случае ошибки пользователей при эксплуатации технических средств, программных средств и систем защиты информации, повлекших нарушение работоспособности проводится анализ и идентификация причин инцидента, определяется ущерб, нанесенный нештатной ситуацией, восстанавливается работоспособность системы.

- В случае обнаружения злоумышленника, неправомерно копирующего, либо изменяющего защищаемую информацию, ответственные специалисты прерывают несанкционированный процесс, блокируют доступ к ИСПДн. Создается комиссия для расследования инцидента.

- При неблагоприятных природных явлениях, стихийных бедствиях все пользователи выключают свои персональные компьютеры. Ответственные специалисты принимают решения о выключении серверов, сетевого оборудования и принимают меры к эвакуации резервных копий с информацией, системных блоков компьютеров, содержащих особо ценную информацию, документов и другого имущества.

3.2 Уровни реагирования на инцидент

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

1. **Незначительный инцидент.** Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на работоспособность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование работниками.
2. **Авария.** Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование работниками.

К авариям относятся следующие инциденты:

отказ элементов ИСПДн и средств защиты из-за повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей; неполадки, связанные с перепадами напряжения в сети электропитания.

3. **Катастрофа.** Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа.

Обычно к катастрофам относят обстоятельства непреодолимой силы, которые могут привести к работоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты: пожар в здании; взрыв; просадка грунта с частичным обрушением здания.

4. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении нештатных ситуаций

4.1. Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства системы, используемые для предотвращения возникновения нештатных 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 средства пожаротушения; системы вентиляции и кондиционирования; системы резервного питания.

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

4.2 Организационные меры

Ответственные за реагирование работники ознакомляют всех работников Учреждения, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий трех рабочих дней с момента выхода нового работника на работу.

Должностные лица 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 лицами, ответственными за реагирование работника на нештатную ситуацию;
- выключение оборудования, электричества, водоснабжения, газоснабжения.

Ответственные работники должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания должностных лиц по реагированию на нештатные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении нештатной ситуации.

Приложение № 1

Источники угроз

Технологические угрозы	
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
Стихийные бедствия	
1	Удар молнии
2	Сильные морозы
3	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
Угрозы, связанные с внешними поставщиками	
1	Отключение электроэнергии
2	Физически разрыв внешних каналов связи
Угроза, связанная с человеческим фактором	
1	Ошибка персонала, имеющего доступ к серверной
2	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Иные угрозы	
1	Сбой технических средств ИСПДн
2	Сбой информационных систем или программного обеспечения