УТВЕРЖДАЮ

Генеральный Директор
ООО УК «Петровская Слобода»

_____
Шахов П.П.
01.12.2018
М.П.

Инструкция
пользователя информационной системы персональных данных при возникновении нештатных ситуаций

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных систем персональных данных ООО УК «Петровская Слобода» (далее – ИСПДн), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

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

2. 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 срок, не превышающий 3х 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 учета 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 несет ответственный за организацию обработки персональных данных. Генеральный Директор ООО УК «Петровская Слобода» 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 дождем;

— 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.