Утверждено
Приказом и.о.генерального директора
Фонда капитального ремонта ВО
от 18.12.2018 № 110/5

ИНСТРУКЦИЯ
о порядке действий во внештатных ситуациях и восстановлению после сбоя

1. Общие положения

Настоящая Инструкция устанавливает порядок действий во внештатных ситуациях и действий сотрудников некоммерческой организации «Фонд капитального ремонта многоквартирных домов Владимирской области» (далее Фонд).

Целью настоящей Инструкции является определение основных мер, методов и средств сохранения (поддержания) работоспособности ИСПДн при возникновении различных внештатных ситуаций, а также способов и средств восстановления информации и процессов ее обработки в случае нарушения работоспособности ИСПДн и ее основных компонентов.

2. Общие требования

Источники информации о возникновении внештатной ситуации:

– пользователи, обнаружившие подозрительные изменения в работе или конфигурации системы или средств ее защиты в своей зоне ответственности;
– средства защиты, обнаружившие кризисную ситуацию;
– системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения кризисной ситуации.

Все пользователи, работа которых может быть нарушена в результате возникновения угрожающей или серьезной внештатной ситуации, должны немедленно устно оповещаться ответственным за организацию обработки персональных данных (ПДн). Дальнейшие действия по устранению причин нарушения работоспособности информационной системы персональных данных (ИСПДн), возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями персонала и пользователей системы.

Каждая внештатная ситуация должна анализироваться ответственным за организацию обработки ПДн. По результатам этого анализа должны вырабатываться предложения по изменению полномочий пользователей, атрибутов доступа к ресурсам, созданию дополнительных резервов, изменению конфигурации системы или параметров настройки средств защиты и т.п., при необходимости должно проводиться расследование причин ее возникновения, оценка причиненного ущерба, определение виновных и принятие соответствующих мер.

Серьезная и угрожающая внештатная ситуация могут требовать оперативной замены и ремонта вышедшего из строя оборудования, а также восстановления поврежденных программ и наборов данных из резервных копий.

Оперативное восстановление программ (используя эталонные копии) и данных (используя страховые копии) в случае их уничтожения или порчи в серьезной или угрожающей кризисной ситуации обеспечивается резервным (страховым) копированием и внешним (по отношению к основным компонентам системы) хранением копий. Внешнее хранение подразумевает нахождение копий в выделенных хранилищах (сейфах), находящихся в специально отведенных помещениях.

Резервному копированию подлежат все программы и данные, обеспечивающие работоспособность и выполнение задач системы (системное и прикладное программное обеспечение, базы данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д.

Все программные средства, используемые в системе должны иметь эталонные (дистрибутивные) копии.

Необходимые действия персонала по созданию, хранению и использованию резервных копий программ и данных должны быть отражены в функциональных обязанностях соответствующих категорий персонала – начальник отдела информационно-технического обеспечения и ответственный за организацию обработки ПДн.

3. Меры обеспечения непрерывной работы и восстановления

Технические меры:

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения внештатных ситуаций, такие как:

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

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

– локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
– источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
– дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т.д.);
– резервные линии электропитания в пределах комплекса зданий;

- аварийные электрогенераторы.

Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

Организационные меры

Резервное копирование и хранение данных (для обрабатываемых ПДн, для технологической информации, эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн должно осуществляться автоматически один раз в день.

Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

Носители должны храниться не менее года для возможности восстановления данных.

4. Действия персонала при возникновении внештатных ситуаций

Сотрудник, обнаруживший сбой в работе ИСПДн в результате внештатной ситуации, должен незамедлительно поставить в известность ответственного за организацию обработки ПДн.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственный за организацию обработки ПДн совместно с начальником отдела информационно-технического обеспечения предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.