Приложение № 10
к приказу Комитета по внешним
связям Санкт-Петербурга
от 27.01.2015 № 1-П

ИНСТРУКЦИЯ
о порядке резервного копирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных в Комитете по внешним связям Санкт-Петербурга

1. Назначение и область действия

Порядок резервного копирования и восстановления работоспособности технических средств (далее – ТС) и программного обеспечения (далее – ПО), баз данных и средств защиты информации (далее – СЗИ) определяет действия (далее – Инструкция), связанные с функционированием информационных систем персональных данных (далее – ИСПДн) в Комитете по внешним связям Санкт-Петербурга (далее – Комитет), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачей данной Инструкции является:

определение мер защиты от потери информации;

определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех государственных гражданских служащих и работников, замещающих должности, не являющиеся должностями государственной гражданской службы Комитета (далее – пользователи), имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

2. Порядок реагирования на инцидент

В Инструкции под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:

в результате непреднамеренных действий пользователей;

в результате преднамеренных действий пользователей и третьих лиц;

в результате нарушения правил эксплуатации технических средств ИСПДн;

в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

В случае совершения инцидента, в кратчайшие сроки, не превышающие одного рабочего дня, администратор безопасности ИСПДн и пользователь ИСПДн с привлечением уполномоченных сотрудников службы технической поддержки Санкт-Петербургского государственного унитарного предприятия «Санкт-Петербургский информационно-аналитический центр» (тел. 576-68-30, 576-60-66) предпринимают меры по восстановлению работоспособности информационной системы. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, 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 Комитета (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

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.

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

3.2 Организационные меры

Резервное копирование и хранение данных должно осуществляться на периодической основе:

для обрабатываемых персональных данных – не реже раза в неделю;

для технологической информации – не реже раза в месяц;

Данные о проведении процедуры резервного копирования, должны отражаться в специально созданном журнале учета согласно приложению.

Носители, на которые произведено резервное копирование, должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

4. Ответственность

Ответственным за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор безопасности информации Комитета.

Ответственность за поддержание установленного в Инструкции порядка проведения резервного копирования и баз данных в ИСПДн возлагается на пользователей ИСПДн Комитета.

Приложение
к Инструкции о порядке резервного
копированиями и восстановления
работоспособности технических средств
и программного обеспечения, баз данных
и средств защиты информации
информационных систем персональных
данных в Комитете по внешним связям
Санкт-Петербурга

ЖУРНАЛ
учета записей резервных копий

№ записи	ИСПДн	Дата создания резервной копии	Наименование носителя	ФИО, должность лица, осуществившего резервное копирование	Подпись должностного лица, осуществившего резервное копирование