УТВЕРЖДАЮ:
И.о. директора ГБПОУ СПЦ №5
_____ Н.В. Колесникова
«02» декабря 2014г.

Порядок
резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационной системы персональных данных «Сетевой город. Профессиональное образование» государственного бюджетного профессионального образовательного учреждения «Сахалинский политехнический центр №5»

1. Назначение и область действия

Порядок резервирования и восстановления работоспособности технических средств (далее – ТС) и программного обеспечения (далее – ПО), баз данных и системы защиты информации (далее – Порядок), определяет действия, связанные с функционированием автоматизированной информационной системы персональных данных «Сетевой город. Профессиональное образование» (далее – АИС СГПО), используемой в государственном бюджетном профессиональном образовательном учреждении «Сахалинский политехнический центр №5» (далее – ГБПОУ СПЦ №5), меры и средства поддержания непрерывности работы и восстановления работоспособности АИС СГПО.

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

Задачей данного Порядка является:

- ✓ определение мер защиты от потери информации;
- ✓ определение действий восстановления в случае потери информации.

Действие настоящего Порядка распространяется на всех пользователей ГБПОУ СПЦ №5, имеющих доступ к ресурсам АИС СГПО, а также 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.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже 1 раза в 2,5 года.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Администратор АИС СГПО.

Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Ответственный специалист по организации защиты информации.

2. Порядок реагирования на инцидент

В настоящем документе под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов АИС СГПО, предоставляемых пользователям, 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 АИС СГПО;
- ✓ в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на инцидент должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники ГБПОУ СПЦ №5 (Администратор АИС СГПО. Ответственный специалист по организации защиты информации), предпринимают меры по восстановлению работоспособности. 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.

Все критичные помещения ГБПОУ СПЦ №5 (помещения, в которых размещаются элементы АИС СГПО и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

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

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы АИС СГПО, 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 АИС СГПО при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов АИС СГПО 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.).

3.2. Организационные меры

Резервное копирование и хранение данных должно осуществляться на периодической основе, ответственными лицами, назначенными приказами:

- ✓ для обрабатываемых персональных данных – не реже раза в неделю;
- ✓ для технологической информации – не реже раза в месяц;
- ✓ эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы АИС СГПО – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

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

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

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

Носители должны храниться не менее года (для возможности восстановления данных).

Порядок рассмотрен, согласован
на заседании Общего собрания
Протокол от 24 ноября 2014г.