УТВЕРЖДАЮ
Директор колледжа
_____ Э.Т. Ахметова
подпись
«03» ноября 2017 г.

Министерство образования и науки
Республики Татарстан

Государственное автономное
профессиональное образовательное учреждение
«Технический колледж им. В.Д. Поташова»
(ГАПОУ «Технический колледж
им. В.Д. Поташова»)

ИНСТРУКЦИЯ
о резервировании и восстановлении работоспособности технических средств и программного обеспечения, баз данных и средств защиты персональных данных в ГАПОУ «Технический колледж им. В.Д. Поташова»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция о резервировании и восстановлении работоспособности технических средств (далее – ТС) и программного обеспечения (далее – ПО), баз данных и средств защиты персональных данных (далее - СЗПДн) (далее – Инструкция) в ГАПОУ «Технический колледж им. В.Д. Поташова» (далее – Колледж) определяет действия, связанные с функционированием технических и программных средств автоматизированных информационных систем (далее - АИС) и систем защиты персональных данных (далее – СЗПДн).

1.2. Настоящая инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.

1.3. Целью данной инструкции является превентивная защита элементов АИС и СЗПДн от предотвращения потери защищаемой информации.

1.4. Задачами данной инструкции являются:

- определение мер защиты от потери информации;
- определение действий восстановления технических и программных средств АИС и СЗПДн в случае потери информации.

1.5. Действие настоящей инструкции распространяется на всех пользователей, имеющих доступ к ресурсам АИС, в том числе на ответственного за обеспечение безопасности персональных данных информационных систем персональных данных и администратора АИС (далее

– администратор системы), имеющих доступ к техническим и программным средствам СЗПДн в рамках своих полномочий, при возникновении аварийных ситуаций, в том числе:

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

1.6. Пользователями АИС (далее – Пользователь) являются сотрудники структурных подразделений, участвующих в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки персональных данных (далее – ПДн) и имеющих доступ к аппаратным средствам, программному обеспечению, данным и СЗИ АИС .

1.7. Под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов АИС или СЗПДн, предоставляемых пользователям, а также потерей защищаемой информации.

2. ПОРЯДОК РЕАГИРОВАНИЯ НА ИНЦИДЕНТ

2.1. 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 и СЗПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.2. В кратчайшие сроки, не превышающие одного рабочего дня ответственный за обеспечение безопасности персональных данных информационных систем персональных данных и администратор системы предпринимают меры по восстановлению работоспособности.

2.4. Предпринимаемые меры, по возможности, согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. ТЕХНИЧЕСКИЕ МЕРЫ

3.1. 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 АИС;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

3.2. Системы жизнеобеспечения АИС включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

3.3. Все критичные помещения колледжа (помещения, в которых размещаются элементы АИС и СЗПДн) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

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

3.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы АИС и СЗПДн, сетевое и коммуникационное оборудование, а также наиболее критичные АРМ 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, активное сетевое оборудование и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

3.6. Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

3.7. Для обеспечения отказоустойчивости критичных компонентов АИС при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации.

3.8. Для наиболее критичных компонентов АИС должны использоваться территориально удаленные системы кластеров.

3.9. 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.

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

4. ОРГАНИЗАЦИОННЫЕ МЕРЫ

4.1. Резервное копирование и хранение данных должно осуществляться на периодической основе:

- для обрабатываемых ПДн – согласно инструкции по обеспечению безопасности ПДн;
- для технологической информации – не реже раза в месяц;

- эталонные копии программного обеспечения (ОС, штатное и специальное ПО, программные СЗИ), с которых осуществляется их установка на элементы АИС – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

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

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

СОГЛАСОВАНО:

Заместитель директора по информатизации и инновациям — Г.Н. Фаттахова

Начальник отдела кадров — Р.З. Гатина

Ведущий юрисконсульт — Д.Р. Гарафов