П-127/2019

Министерство образования и науки Самарской области
ГБПОУ «ТК им. Н.Д. Кузнецова»

Протокол заседания Совета Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета обучающихся
Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета родителей
Учреждения
от 29.10.2019г. № 20

УТВЕРЖДАЮ
Директор
ГБПОУ «ТК им. Н.Д. Кузнецова»
_____А.Н. Сакеев
«29» октября 2019г.

Приказ № 522 о/д от 29.10.2019

Положение (инструкция) о резервировании и восстановлении работоспособности технических средств (ТС) и программного обеспечения (ПО), баз данных и средств защиты персональных данных (СЗПДн)

1. Общие положения

1.1. Настоящее положение о резервировании и восстановлении работоспособности технических средств и программного обеспечения, баз данных и средств защиты персональных данных (далее - Положение) определяет действия, связанные с функционированием информационных систем персональных данных (далее - ИСПДн) ГБПОУ «ТК им. Н.Д. Кузнецова» (далее - Учреждение), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Настоящее Положение разработано в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»,
- Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»,
- Постановлением Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных",
- Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,
- Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.3. Целью настоящего Положения является порядок резервирования и восстановление работоспособности элементов ИСПДн и меры предотвращения потери

защищаемой информации.

1.4. Задачей данной Инструкции является:

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

1.5. Действие настоящей Инструкции распространяется на всех пользователей Управления, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения ИСПДн;
- системы резервного копирования и хранения данных.

1.6. Ответственным работником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Администратор информационной безопасности.

1.7. Ответственным работником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Администратор информационной безопасности.

2. Порядок реагирования на инцидент.

2.1. В настоящем Положении под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

2.2. 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.

2.3. Реагирование на инцидент включает следующие этапы:

- выявление инцидента;
- анализ и принятие решений;
- принятие мер (технических и организационных) по устранению инцидента.

2.4. В сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Учреждения (Администратор информационной безопасности) 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.

2.5. Порядок восстановления работоспособности ИСПДн.

2.5.1. Восстановление работоспособности ИСПДн осуществляется в случаях, указанных в пункте 2.2 настоящей инструкции.

2.5.2. Восстановление работоспособности ИСПДн осуществляется Администратором информационной безопасности в соответствии с эксплуатационной документации на программное обеспечение и технические средства обработки персональных данных

2.5.3. В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на ответственного за организацию работ по обеспечению безопасности персональных данных..

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

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

3.2. Все критичные помещения Учреждения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.3. 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.

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

- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т.д.).
- Системы обеспечения отказоустойчивости:
- кластеризация;
- технология RAID.

3.5. 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.

3.6. 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.

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

3.8. Резервное копирование и хранение данных осуществляется на периодической основе:

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

3.9. Данные о проведение процедуры резервного копирования отражаются в специально созданном журнале учета.

3.10. Носители, на которые произведено резервное копирование, нумеруются: номером носителя, датой проведения резервного копирования.

3.11. Носители хранятся в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

3.12. Носители хранятся не менее года, для возможности восстановления данных

Положение вступает в силу с момента его утверждения.

В случае необходимости в Положение могут вноситься изменения и дополнения по

согласованию с Советом учреждения.

Разработчик:
заместителя директора по общим вопросам

_____/ Ю.Ю. Алексеев /