ЧАСТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СТАВРОПОЛЬСКИЙ КООПЕРАТИВНЫЙ ТЕХНИКУМ»

СОГЛАСОВАНО
Протокол заседания
Студенческого совета
от «30» августа 2023 г. № 1
Председатель Совета
_____

УТВЕРЖДАЮ
Директор Частного профессионального
образовательного учреждения
«Ставропольский кооперативный техникум»
_____ А.А. Намитоков
от «30» августа 2023 г. Приказ № 112

ИНСТРУКЦИЯ

по организации резервного копирования, восстановления работоспособности технических средств, программного обеспечения и средств защиты информации в информационной системе персональных данных «Автоматизированное рабочее место оператора УОП»

1 Общие положения

1.1 Настоящая инструкция определяет действия, связанные с функционированием информационной системы персональных данных «Автоматизированное рабочее место оператора УОП» (далее - ИСПДн), меры и средства поддержания непрерывности работы и восстановления работоспособности технических средств и программного обеспечения и средств защиты информации.

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

1.3 Задачей данной Инструкции является:

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

1.4 Действие настоящей Инструкции распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн, а также на 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.

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

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

2 Порядок организации резервного копирования в ИСПДн

2.1 Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности ИСПДн в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

2.2 Резервное копирование и хранение данных должно осуществлять на периодической основе:

2

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

2.2 Резервному копированию подлежит информация следующих основных категорий:
- персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений);
- информация, обрабатываемая пользователями в ИСПДн, а также информация, необходимая для восстановления работоспособности ИСПДн, в т.ч. общего пользования и справочно-информационные системы общего использования;
- рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения ИСПДн;

регистрационная информация системы защиты персональных данных ИСПДн;
- другая информация, по мнению пользователей и администраторов являющаяся критичной для работоспособности ИСПДн.

2.3 Резервное копирование информации настраивается и производится под контролем Администратора безопасности однократно после подготовки ИСПДн к работе и хранится:
- одна копия - на локальном жестком диске;
- вторая копия - на отчуждаемом учтенном носителе.

2.4 Резервное копирование защищаемой информации (ПДн) производится еженедельно администратором безопасности ИСПДн.

2.5 После окончания процесса резервного копирования полученную резервную копию (архив) следует скопировать на отчуждаемый учтенный носитель.

2.6 При втором и последующих резервных копированиях текущего месяца возможно создание инкрементных архивов (если данная возможность предусмотрена в средствах резервного копирования).

2.7 В случае нехватки свободного дискового пространства для сохранения файла архива следует удалить наиболее старый архив.

2.8 На отчуждаемом носителе должны храниться архивы не менее чем за два месяца: текущий и предыдущий.

2.9 В случае необходимости восстановления данных из резервной копии, для восстановления следует использовать наиболее поздний архив. В случае невозможности использования наиболее позднего архива по каким-либо причинам, архив, используемый для восстановления, выбирается совместным решением администратора и ответственного за обеспечение безопасности персональных данных.

2.10 Данные о проведении процедуры резервного копирования, должны отражаться в специально созданном Журнале учета проведения процедур резервного копирования в ИСПДн (Приложение 1).

2.11 Машинные носители информации, на которые произведено резервное копирование, должны быть учтены в Журнале учета машинных носителей для архивного

копирования в ИСПДн (Приложение 2), который находится у Администратора безопасности. В случае неотделимости носителей архивной информации от системы резервного копирования допускается их не маркировать и учитывать всю систему как одно целое.

2.13 Физический доступ к архивным копиям предоставляется только Администратору ИСПДн и Администратору безопасности.

2.14 Передача машинных носителей с архивными копиями кому бы то ни было без документального оформления не допускается.

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

2.16 Носители должны храниться не менее одного месяца, для возможности восстановления данных.

2.17 Уничтожение отделяемых машинных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

2.18 На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, осуществляется ежедневное копирование информации, подлежащей резервированию.

2.19 В случае необходимости восстановление данных из резервных копий производится Администратором ИСПДн или Администратором безопасности.

2.20 Восстановление данных из резервных копий происходит в случае их исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

2.21 Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

2.22 Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

2.23 При частичном нарушении или исчезновении записей данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

3. Ответственность

Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением настоящей Инструкции, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на Администратора безопасности ИСПДн.