Утверждено:
Приказом Генерального директора
ООО «УЭЦ «СБ»
от «30» декабря 2021 г. № 56

Правила резервного копирования и восстановления электронных документов

1. Общие положения

1.1. Настоящие Правила резервного копирования и восстановления электронных документов (далее – Правила) разработано в соответствии с требованиями:

- Федерального закона от 22.10.2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;
- Приказа Федерального архивного агентства от 20 декабря 2019 года № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»;
- Федерального закона от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.2 Целью резервного копирования является предотвращение потери информации на бумажных носителях, потери информации при сбоях оборудования, программного обеспечения, в критических и кризисных ситуациях и т.д.

1.3. Правила вступают в силу с момента утверждения и действует без ограничения срока (до внесения соответствующих изменений и дополнений или принятия нового Положения).

2. Порядок проведения резервного копирования электронных документов

2.1. Резервное копирование производиться в автоматическом режиме не реже одного раза в сутки в ночной период времени. Допускается проводить резервное копирование в автоматическом в иное время - время наименьшей загрузки сервера.

2.2. Резервное копирование производиться в сетевое хранилище NAS. Если потребуется дополнительная защита, данные могут быть также сохранены на переносных USB-дисках и флэшках, или в облачное хранилище, подключаемых к NAS.

2.3. Резервному копированию подлежит информация следующих основных категорий:

Персональная информация пользователей (личные каталоги на файловых серверах);

Групповая информация пользователей (общие каталоги отделов);

Информация, необходимая для восстановления серверов и систем управления базами данных (далее – СУБД);

Персональные профили пользователей сети;

Информация автоматизированных систем, в т.ч. баз данных;

Рабочие копии установочных компонент программного обеспечения рабочих станций;

Данные с рабочих станций, содержащих критически важную информацию.

3. Контроль результатов резервного копирования

3.1. Не реже одного раза в неделю ответственный специалист обязан визуально убеждаться в наличии свободного места и наличии резервных копий на носителе информации. В случае возникновения непредвиденных ситуаций ответственный специалист должен немедленно сообщить о них Генеральному директору.

3.2. Не реже одного раза в месяц специалист ИТ обязан проводить тестовую проверку целостности копий баз данных.

4. Восстановление данных с резервных копий

4.1. Восстановление утраченных данных производится из резервной копии, обеспечивающей минимальную потерю данных, содержащихся в информационном ресурсе.

4.2. Восстановление файлов из резервной копии редкое действие. Периодическое выполнение проверки возможности восстановления файлов из резервных копий выявит проблемы с процедурами резервного копирования, чтобы была возможность скорректировать их до того, как данные будут потеряны.

4.3. Проверка резервной копии выполняется восстановлением как отдельных папок и файлов, так и всего образа компьютера. Проверка резервных копий осуществляется выборочно не реже одного раза в два месяца.