Приложение № 8

Утверждено
приказом КОГОАУ ВГГ
от 15.02.2024 № 39/1

ПОЛОЖЕНИЕ
по резервированию и восстановления работоспособности технических средств, программного обеспечения, баз данных и средств защиты информации

г. Киров,
2024 г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

КИРОВСКОЕ ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ "ВЯТСКАЯ ГУМАНИТАРНАЯ ГИМНАЗИЯ С УГЛУБЛЕННЫМ ИЗУЧЕНИЕМ АНГЛИЙСКОГО ЯЗЫКА", Вологжанина Валерия Владимировна, Директор гимназии

06.04.24 11:03 (MSK)

Сертификат 18E1DDD07A8141A407968B494A7DD012

Содержание

1. Общие положения

1.1. Назначение

Настоящее Положение устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в базах данных на серверах, а также к резервированию аппаратных средств в Кировском областном государственном общеобразовательном автономном учреждении «Вятская гуманитарная гимназия с углубленным изучением английского языка» (Далее - Гимназия).

Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности информационных систем персональных данных, информационных ресурсов, средств обработки информации в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

1.2. Цель разработки

Настоящее Положение разработано с целью:

- определения условий обеспечения возможности восстановления информационных систем персональных данных, информационных ресурсов, средств обработки информации после аварий и нештатных ситуаций;
- упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации;
- обеспечения защиты прав субъектов персональных данных.

1.3. Область применения

Настоящий документ применяется:

- к процессам эксплуатации информационных систем персональных данных, информационных ресурсов и средств обработки информации.

1.4. Срок действия и порядок внесения изменений

Положение действует с момента утверждения и действует бессрочно до замены новой версией или документом, его заменяющим.

Документ подлежит регулярному пересмотру с периодичностью не реже 1 раза в 3 года, а также в случае изменения требований законодательства, требований со стороны партнеров, изменения оценки рисков информационной безопасности. Изменения в Положение вносятся путем издания новой версии и ознакомления с ним сотрудников.

Срок хранения после прекращения действия: постоянно.

1.5. Используемые сокращения

БД - база данных;
ИБ – информационная безопасность;
ИСПДн – информационная система персональных данных;
ИТ – информационные технологии;
ПДн – персональные данные;
СКЗИ – средства криптографической защиты информации.

2. Порядок резервного копирования

2.1. Общие сведения

2.1.1. Резервному копированию подлежит информация следующих основных категорий:

- информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений) на файловых серверах;

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
КИРОВСКОЕ ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ "ВЯТСКАЯ ГУМАНИТАРНАЯ ГИМНАЗИЯ С УГЛУБЛЕННЫМ ИЗУЧЕНИЕМ АНГЛИЙСКОГО ЯЗЫКА", Вологжанина Валерия Владимировна, Директор гимназии
06.04.24 11:03 (MSK)
Сертификат 18E1DDD07A8141A407968B494A7DD012

- информация, обрабатываемая пользователями в информационных системах персональных данных и информационных ресурсах;
- базы данных (БД);
- конфигурация и дистрибутивы системного программного обеспечения для развертывания на серверы;
- образы систем и информация сервисов инфраструктуры;
- образы систем и информация сервисов и средств информационной безопасности;
- конфигурация сетевого оборудования;
- другая информация, являющаяся критичной для работоспособности информационных систем персональных данных и информационных ресурсов.

2.1.2. Резервное копирование осуществляется в соответствии с Регламентом, приведенным в Приложении 1 (далее – Регламент).

2.1.3. Допускается применение автоматизированной системы резервного копирования с учетом Регламента.

2.1.4. Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений.

2.1.5. Резервные копии должны храниться на отдельных от средств вычислительной техники носителях в отдельном помещении.

2.1.6. Резервные копии при передаче по каналам, выходящим за пределы контролируемой зоны, должны передаваться с использованием сертифицированных средств криптографической защиты информации.

2.1.7. Доступ к резервным копиям имеют:

- руководитель организации;
- Ответственный за информационную безопасность;
- Администратор информационной безопасности;
- Системный администратор.

2.1.8. Доступ к резервным копиям должен журналироваться средствами системы хранения резервных копий. Информация журнала событий безопасности должна храниться не менее 1 года.

2.1.9. О выявленных попытках несанкционированного доступа к резервируемой информации и аппаратным средствам, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается в директору Гимназии служебной запиской в течение рабочего дня после обнаружения указанного события.

2.2. Общие требования к резервному копированию

2.2.1. Резервное копирование производится при помощи специализированных программно-аппаратных систем резервного копирования, состав которых обеспечивает выполнение требований Регламента резервного копирования и необходимые требования безопасности информации.

2.2.2. Сопровождение системы резервного копирования возлагается Системного администратора, который обязан следить за работоспособностью программных и аппаратных средств системы.

2.2.3. Учет носителей информации, применяемых для хранения архивов производится согласно Порядку обращения с носителями информации. Все съемные носители информации с архивными копиями маркируются, на них указывается предназначение носителя.

2.2.4. Носители, устанавливаемые для долгосрочной работы в составе системы резервного копирования, учитываются в Журнале учета машинных носителей информации перед установкой в систему.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
КИРОВСКОЕ ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ "ВЯТСКАЯ ГУМАНИТАРНАЯ ГИМНАЗИЯ С УГЛУБЛЕННЫМ ИЗУЧЕНИЕМ АНГЛИЙСКОГО ЯЗЫКА", Вологжанина Валерия Владимировна, Директор гимназии
06.04.24 11:03 (MSK)
Сертификат 18E1DDD07A8141A407968B494A7DD012

2.2.5. Машинные носители информации, содержащие резервные копии утилизируются в соответствии с Порядком уничтожения персональных данных.

2.3. Ответственность за состояние резервного копирования

2.3.1. Ответственность за периодичность и полноту резервного копирования, а также состояние системы резервного копирования возлагается на Системного администратора.

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

2.3.3. В случае обнаружения попыток несанкционированного доступа к носителям архивной информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, информация об этом сообщается в Ответственному за информационную безопасность служебной запиской в течение 24 часов.

2.4. Контроль результатов резервного копирования

2.4.1. Контроль результатов всех процедур резервного копирования осуществляется Системным администратором ежедневно. Отчет о результатах направляется Ответственному за информационную безопасность ежедневно.

2.4.2. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, осуществляется ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения. При этом обеспечиваются необходимые меры ограничения доступа и защиты таких серверов.

2.5. Ротация носителей резервной копии

2.5.1. Система резервного копирования обеспечивает возможность периодической ротации резервных носителей без потерь информации на них, а также обеспечивает восстановление текущей информации информационных систем персональных данных в случае отказа любого из устройств резервного копирования.

2.5.2. Все процедуры по ротации носителей из системы резервного копирования осуществляются Системным администратором.

2.5.3. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек. При этом перед повторным использованием носителя на нем должно быть выполнено гарантированное стирание данных.

2.5.4. Не допускается использовать носители информации дольше 4 лет.

2.5.5. Информация с носителей, которые перестают использоваться в системе резервного копирования, уничтожается в соответствии с Порядком уничтожения персональных данных.

2.6. Восстановление информации из резервных копий

2.6.1. При необходимости восстановление данных из резервных копий производится Системным администратором.

2.6.2. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев. В таких случаях решение о восстановлении принимается Системным администратором и Ответственным за информационную безопасность по итогам анализа инцидента информационной безопасности.

2.6.3. Восстановление системного программного обеспечения, программного обеспечения общего назначения и их настроек на серверах производится из резервных копий.

2.6.4. Восстановление данных выполняется исходя из определенной в регламенте схемы резервного копирования.

Приложение 1

Регламент резервного копирования

№	Типа резервируемого объекта	Периодичность и тип резервного копирования	Срок хранения копий	Допустимый период, за который данные могут быть потеряны
1.	База данных	24 часа - полное	Ежедневные – 1 неделя Еженедельные – 1 месяц Ежемесячные – 3 месяца	24 часа
2.	Общие сетевые ресурсы	24 часа - полное	Ежедневные – 1 неделя Еженедельные – 1 месяц Ежемесячные – 3 месяца	24 часа
3.	Серверы (системные разделы)	При изменении конфигурации - полное	3 последних копии	-
4.	Контроллеры домена, серверы безопасности	24 часа – полное	Ежедневные – 1 неделя Еженедельные – 1 месяц Ежемесячные – 3 месяца	4 часа
5.	Виртуальные машины	24 часа – полное	Ежедневные – 1 неделя Еженедельные – 1 месяц Ежемесячные – 3 месяца	24 часа
6.	Журналы безопасности, журналы резервных копий	24 часа	1 год	4 часа

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
КИРОВСКОЕ ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ "ВЯТСКАЯ ГУМАНИТАРНАЯ ГИМНАЗИЯ С УГЛУБЛЕННЫМ ИЗУЧЕНИЕМ АНГЛИЙСКОГО ЯЗЫКА", Вологжанина Валерия Владимировна, Директор гимназии
06.04.24 11:03 (MSK)
Сертификат 18E1DDD07A8141A407968B494A7DD012