Тип работы: Дипломная работа

Предмет: Информационные технологии

Содержание

ВВЕДЕНИЕ

В рамках данной работы проведена разработка проекта внедрения системы резервного копирования в деятельность организации. Задачи организации резервного копирования обеспечивают возможность сохранения информационных ресурсов при возникновении сбоев технического характера. Для каждого из информационных ресурсов в зависимости от частоты актуализации разрабатывается регламент сохранения на внешние носители, порядок обеспечения хранения, назначаются ответственные специалисты, разрабатываются регламенты защиты от утечек, вызванных утерями или попытками получения несанкционированного доступа к носителям информации.
Оперативное восстановление работоспособности системы сокращает время технологического простоя в работе организаций, сокращая потери, ими вызванные.
Причинами для проведения операций по восстановлению баз данных могут быть: вирусная активность, аппаратный сбой, ошибочные действия администратора, форс-мажорные обстоятельства.
Таким образом, для обеспечения возможности восстановления работоспособности информационных систем компаний необходима разработка регламента проведения резервного копирования, включающего:
- описание порядка проведения резервного копирования и восстановления данных;
- определение порядка хранения носителей информации, содержащих резервные копии информационных ресурсов;
- определение технологии проведения операций по резервному копированию (через использование встроенных средств резервирования, либо с использованием сторонни).
Таким образом, вопросы регламентации проведения операций резервного копирования также являются актуальными, так как при отсутствии упорядоченности процесса резервирования процесс восстановления работоспособности будет максимально затруднен.

Целью данной работы является создание регламентов политики резервного копирования информации на примере ООО «Альфа-Телеком».
Задачи работы:
- анализ проблематики проведения резервного копирования;
- анализ технологий организации резервного копирования, порядка хранения носителей информации;
- изучение функционала программных и технических средств, используемых для выполнения операций резервного копирования;
- разработка проекта внедрения системы резервного копирования в условиях исследуемой компании;
- оценка вложений в реализацию проекта.
Объект исследования: технологии информационной безопасности в условиях ООО «Альфа-Телеком».
Предмет исследования: организация системы резервного копирования в условиях компании.

ГЛАВА 1. АНАЛИЗ ТРЕБОВАНИЙ К ПРОВЕДЕНИЮ ОПЕРАЦИЙ РЕЗЕРВНОГО КОПИРОВАНИЯ ДАННЫХ

1.1 Актуальность использования технологий копирования и восстановления информации

Резервное копирование данных — процесс создания копии данных на носителе, предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения. На сегодняшний день информационные ресурсы компаний представляют собой актив, ценность которого является достаточно высокой, что объясняется тем, что большинство бизнес-процессов связаны с использованием систем автоматизации, наличием тенденций отказа от документооборота на бумажных носителях. Утеря информации может привести к значительным убыткам организаций, связанным с необходимостью простоев в работе специалистов, поиску возможностей восстановления информации из различных источников. Для минимизации вероятности утери данных в организациях разрабатываются регламенты резервного копирования, пори соблюдении которых возможно восстановление информации при возникновении сбоев технического характера. Регламентация технологии резервного копирования осуществляется в соответствии со спецификой обрабатываемой информации, частотой ее актуализации. Таким образом, задача обеспечения сохранности данных, находящихся на различного рода накопителях, приобретает особую актуальность.
В рамках данной работы проведен анализ законодательных актов, регламентирующих вопросы обеспечения защиты информации. Перечень нормативных актов указанного класса содержит документы:
- 152- ФЗ «О Персональных данных» от 27.07.2006;
- 149 – ФЗ «Об информации, информационных технологиях и защите информации» от 27.07.2006;
- Статьи Трудового кодекса, кодекса об административных правонарушениях;
- Документы ФСБ, ФСТЭК, Роскомнадзора.

В рамках работы с информацией, относящейся к категории конфиденциальных сведений, необходимо проведение классификации обрабатываемых данных, определение перечня мер в области обеспечения защиты информации, создание организационной структуры, принятие мер организационного, инженерно-технического характера.
Целью мероприятий по обеспечению защиты информации является обеспечение конфиденциальности, доступности, целостности. Компания, осуществляющая обработку конфиденциальных данных, должна обеспечивать защищенность от утечек, несанкционированного доступа, копирования и распространения информации.
Объектами защиты информации, находящимися на жестких дисках, могут быть [13]:
- базы данных программных комплексов;
- документы, используемые в рамках деятельности компании;
- мультимедиа-материалы;
- графические файлы;
- закрытые ключи электронной подписи, хранящиеся в реестре;
- пользовательские настройки к программным комплексам;
- резервные копии различного рода данных;
- архивы баз данных.

Также данные, находящиеся на жестких дисках, могут включать конфиденциальную информацию различного типа (персональные данные, коммерчески значимую информацию, информацию об архитектуре информационной безопасности, парольную информацию).

Таким образом, одним из требований к сохранности данных является обеспечение функциональности аппаратной части компьютера, включая накопители на жестких дисках.
Как правило, резервное копирование производится для объектов следующих видов [13]:
• баз данных программных комплексов;
• дистрибутивов прикладного программного обеспечения;
• файлов настроек;
• серверные операционные системы (включая ресурсы Active Directory);
• криптографические системы.
Перечень баз данных, подлежащих сохранению, определяется приказом по организации.
Проведение резервного копирования баз данных прикладных программных комплексов производится для возможности их последующего восстановления при необходимости.
Порядок и технология резервного копирования баз данных зависит от [19]:
 назначения и функциональных особенностей базы данных (важности, изменчивости и т.д.);
 особенностей работы использующих данные ресурсы прикладных программ.
Проведение резервного копирования баз данных может производиться с установленной периодичностью: каждый день, один раз в неделю, в месяц или ежегодно. В зависимости от технологий проведения операций резервного копирования, возможно выполнение полного, дифференциального или инкрементального копирования. Копирование может производиться с проведением архивации данных.
Для определенных баз данных возможна установка специальной периодичности проведения копирования, например, при проведении специальных операций (установки обновлений ПО, изменения структуры БД, выполнения скриптов, сжатия и др.). Разработка технологии проведения дополнительного копирования проводится администраторами баз данных, приложений и защиты информации.
Тип накопителей данных, используемых для хранения резервных копий, зависит от характеристик аппаратно-программных комплексов, использующих информационный ресурс. Количество копий (дублей) определяется из необходимости безусловного обеспечения восстановления информационного ресурса в срок, не приводящий к срыву возложенных на организацию основных задач, который определяется в частной инструкции резервного копирования на ресурс или соответствующим разделом программно-эксплуатационной документации [19].
Правила хранения резервных копий баз данных определяются утвержденными регламентами.
Для защиты от нештатных ситуаций хранение носителей резервных копий баз данных осуществляется в помещении, удаленном от носителей основной базы данных.
За сохранность носителей, содержащих резервные копии информационных ресурсов несут ответственность работники компании, список которых определяется специальным приказом.
Процесс резервного копирования баз данных должен контролироваться специалистами, курирующими вопросы обеспечения информационной безопасности.
Технологии резервного копирования классифицируется по:
- типам
1.2. Организация копирования

Вычислительные средства, применяемые для проведения операций копирования баз данных, по возможности должны устанавливаться удаленно от комплекса, содержащего дублируемый ресурс. Рекомендуется их установка в разных зданиях, либо на разных этажах одного здания.
Инструкция о порядке резервного копирования информационного ресурса, не входящего в общий список, согласовываются с подразделениями, курирующими вопросы защиты информации, подразделением - владельцем ресурса, утверждаются руководством и подлежат актуализации с учетом изменений в составе защищаемых ресурсов, используемых средств, текущих директивных указаний и т.д.
В технологической инструкции, в частности, определяется [19]:
 список резервируемых компонентов информационного ресурса;
 периодичность и технология проведения операций по резервному копированию;
 обоснование необходимости и порядка проведение операций копирования и архивирования;
 число хранимых копий и возможность их тиражирования;
 описание требований к хранению носителей, содержащих резервные копии;
 описание используемых при копировании и тиражировании средств;
 технология документального оформления проведения операций по резервному копированию (ведения журнала учета копирования информационных ресурсов);

 порядок использования резервных копий для восстановления целостности информационных ресурсов;
 порядок документального оформления факта восстановления ресурса с использованием резервных копий;
 порядок актуализации инструкции;
 установление персональной ответственности за выполнение копирования, хранение копий и контроля;
 другие необходимые положения.

Для учета наличия резервных копий целесообразно ведение специального журнала, в котором указывается [19]:

- Дата резервного копирования;
- Наименование информационного ресурса;
- Имя файла резервной копии;
- ФИО сотрудника, проводившего копирование;
- Учетный номер носителя информации, на который проведено резервное копирование;
- Номер кабинета и сейфа, где хранится носитель резервной копии.

Для баз данных, скопированных на выделенные носители информации, предназначенные для хранения резервных копий, необходимо формирование описи хранимых копий баз данных, являющейся отдельной страницей журнала, для ресурсов, не включенных в перечень резервного копирования на сменное сетевое хранилище – отдельный раздел журнала.

Оформление записи в «Журнале учета копирования баз данных» производится специалистами, контролирующими процесс резервного копирования.

1.3. Организация восстановления информационных ресурсов

Восстановление базы данных из резервной копии осуществляется коллегиально (комиссией) с привлечением сотрудников подразделения, ответственного за работу с прикладной системой, ИТ-специалистов и специалистов по информационной безопасности. Состав комиссии определяется приказом руководителя по каждому случаю восстановления ресурса из резервной копии. Членами комиссии по восстановлению информационных ресурсов являются [14]:

 специалисты с правами администратора данного информационного ресурса;

Список использованных источников

1. База данных угроз ФСТЭК. [Электронный ресурс]. Режим доступа: https://bdu.fstec.ru/threat (дата доступа: 27.04.2022)
2. Клименко И. С. Информационная безопасность и защита информации: модели и методы управления: монография / И. С. Клименко. - Москва: ИНФРА-М, 2020. – 178с.
3. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / В.В. Бондарев. - Москва: Изд-во МГТУ им. Н.Э. Баумана, 2018. - 250 с.
4. Солодянников А. В. Комплексная система защиты объектов информатизации: учебное пособие / А. В. Солодянников. - Санкт-Петербург: Изд-во Санкт-Петербургского государственного экономического университета, 2017. - 91 с.
5. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И. С. Клименко. - Москва: ИНФРА-М, 2020. – 178 с.
6. Чекулаева Е. Н., Кубашева Е. С. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. - Йошкар-Ола: Поволжский государственный технологический университет, 2020. - 153 с.
7. Алексеев А. П. Многоуровневая защита информации: монография / А. П. Алексеев. - Самара : ПГУТИ, 2017. - 128 с.
8. Благодаров, А. В. Алгоритмы категорирования персональных данных для систем автоматизированного проектирования баз данных информационных систем / А. В. Благодаров, В.С. Зияутдинов, П.А. Корнев, В.Н. Малыш. - Москва: Горячая линия-Телеком, 2015. - 115 с.
9. Бондарев, В. В. Анализ защищенности и мониторинг компьютерных сетей: методы и средства: учебное пособие / В.В. Бондарев. - Москва: Изд-во МГТУ им. Н.Э. Баумана, 2017. – 225с.
10. Язов Ю. К., Соловьев С. В. Организация защиты информации в информационных системах от несанкционированного доступа : [монография] / Ю. К. Язов, С. В. Соловьев. - Воронеж: Кварта, 2018. - 588 с.
11. Марков А. С. Техническая защита информации: курс лекций: учебное пособие / Марков А.С. - Москва : Изд-во АИСНТ, 2020. – 233с.

12. Королев, Е. Н. Администрирование операционных систем: учебное пособие / Е. Н. Королев. - Воронеж: Воронежский государственный технический университет, 2017. - 85 с.
13. Михайлова, Е. М. Организационная защита информации [Электронный ресурс]/ Михайлова Е. М., Анурьева М. С. - Тамбов: ФГБОУ ВО "Тамбовский государственный университет имени Г. Р. Державина", 2017. – 342 с.
14. Камалова Г. Г. Юридическая ответственность за нарушение конфиденциальности информации: монография / Камалова Гульфия Гафиятовна. - Саратов : Амирит, 2019. - 160 с.
15. Никифоров, С. Н. Защита информации: защита от внешних вторжений : учебное пособие / С.Н. Никифоров. - Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, 2017. - 82 с
16. Белов, Е. Б. Организационно-правовое обеспечение информационной безопасности: учебник / Е.Б. Белов, В.Н. Пржегорлинский. - 2-е изд., испр. и доп. - Москва: Академия, 2020. – 332с.
17. Ревнивых, А. В. Информационная безопасность в организациях: учебное пособие / А. В. Ревнивых. - Новосибирск: НГУЭУ, 2018. - 83 с.
18. Щеглов А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с.
19. Зенков А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с.
20. Васильева И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2022. — 349 с.
21. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с.