МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)
ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ

Кафедра Автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

Организация системы резервного копирования при обеспечении защиты информации в профессиональной образовательной организации

Магистерская диссертация
по направлению: 44.04.04 Профессиональное обучение (по отраслям)
Направленность (профиль): Управление информационной безопасностью в профессиональном образовании
Форма обучения заочная

Проверка на объем заимствований:
79 % авторского текста

Работа рекомендована к защите
«18» 01 2021 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил(а):
Студент(ка) группы ЗФ-309-210-2-1
Шалаев Александр Дмитриевич

Научный руководитель:
Белевитин Владимир Анатольевич, д.т.н, профессор

Челябинск
2021

ОГЛАВЛЕНИЕ

АННОТАЦИЯ

Содержание данной работы представляет собой полную разработку стратегии резервного копирования данных для профильной образовательной организации. Работа будет разделена на теоретическую и практическую части. Первая часть будет содержать теоретические отправные точки для вопроса резервного копирования данных. Практическая часть будет сосредоточена на разработке стратегии резервного копирования данных, включая классификацию данных, рекомендации, интеграцию в организационную структуру компании, проектирование процессов резервного копирования и последующий выбор технологий для их реализации.

ВВЕДЕНИЕ

Для разработки своей магистерской диссертации я выбрал образовательную организацию Южно-Уральский государственный технический колледж, главным образом потому, что я был здесь на , что во многих случаях может привести к значительным потерям конкурентоспособности компании или даже полное прекращение ее деятельности. А на восстановление утерянного методического материала может потребоваться не одна неделя работы. Для этого необходимо в каждой образовательной организации иметь качественную и отлаженную системы резервного копирования данных.

Цель моей магистерской диссертации - разработать подходящую стратегию резервного копирования для компании Южно-Уральский государственный технический колледж, который заменил бы существующий не очень удовлетворительный способ резервного копирования данных.

Теоретическая часть работы будет содержать определение и описание отдельных критериев классификации данных, краткое изложение используемых в настоящее время технологий с указанием их цены, срока службы и др. их достоинства и недостатки.

В практической части я кратко охарактеризую компанию, для которой я обрабатываю это предложение и проанализирую её текущее состояние в области резервного копирования. Затем я разработаю собственное предложение по выходу из ситуации. Я постараюсь выбрать технологии, которые будут использоваться для резервного копирования, так что их общая стоимость не превышала доступную для компании сумму.

Неотъемлемой частью этой работы также будет предложение по организации процесса резервного копирования и информационной

безопасности. Необходимо будет определить, кто и в какой степени отвечает за безопасность данных и определить принципы, которых необходимо будет придерживаться для обеспечения безопасности информации.На основании этих принципов предложить индивидуальные директивы. В конце работы я попытаюсь разработать кризисный план восстановления информации, который будет охарактеризовать процедуры в случае сбоя первичных данных.

ГЛАВА 1. ПОСТАНОВКА ПРОБЛЕМЫ И ЦЕЛЬ РАБОТЫ

1.1 Анализ образовательной организации Южно-Уральский государственный технический колледж

Историческая справка

История машиностроительного техникума тесно связана со становлением такого промышленного гиганта как Челябинский тракторный завод.

В 1930 году был создан Челябинский тракторный техникум, зачислено 120 человек.

В мае 1931 года Тракторный техникум перевели во вновь выстроенное здание школы ФЗУ. Для учебных целей техникуму было отведено семь аудиторий с «…незначительным оборудованием…», под общежитие отведено здание.

В 1940 году техникум занял первое место среди других техникумов Наркомсредмаша СССР, это говорит о высоком качестве не только преподавания, но и оснащения Тракторного техникума.

В 1942 году открылось отделение подготовки специалистов по гусеничным машинам – танкам, и техникум был переименован в машиностроительный. Выпускники тех лет вписали не одну страницу в историю Танкограда, а девятнадцать студентов и преподавателей техникума погибли на фронтах Великой Отечественной войны. После войны учебное заведение обозначило свой вектор развития – подготовка квалифицированных специалистов машиностроительного профиля.

В 1956 году в техникуме открылись вечернее и заочное отделения. В разные годы техникумом руководили И.И. Кириллов, Ю.А. Кузнецов, Г.А. Ярцев

С 1982 года работой коллектива руководил В.В. Баранов. Из стен учебного заведения вышли тысячи выпускников, среди которых известные

общественные деятели, профессора, конструкторы, просто хорошие люди и грамотные специалисты.

7 сентября 2010 — Создание нового учебного заведения – Южно-Уральского государственного технического колледжа (ЮУрГТК) в результате реорганизации Челябинского монтажного колледжа, Челябинского политехнического техникума и Челябинского машиностроительного техникума.

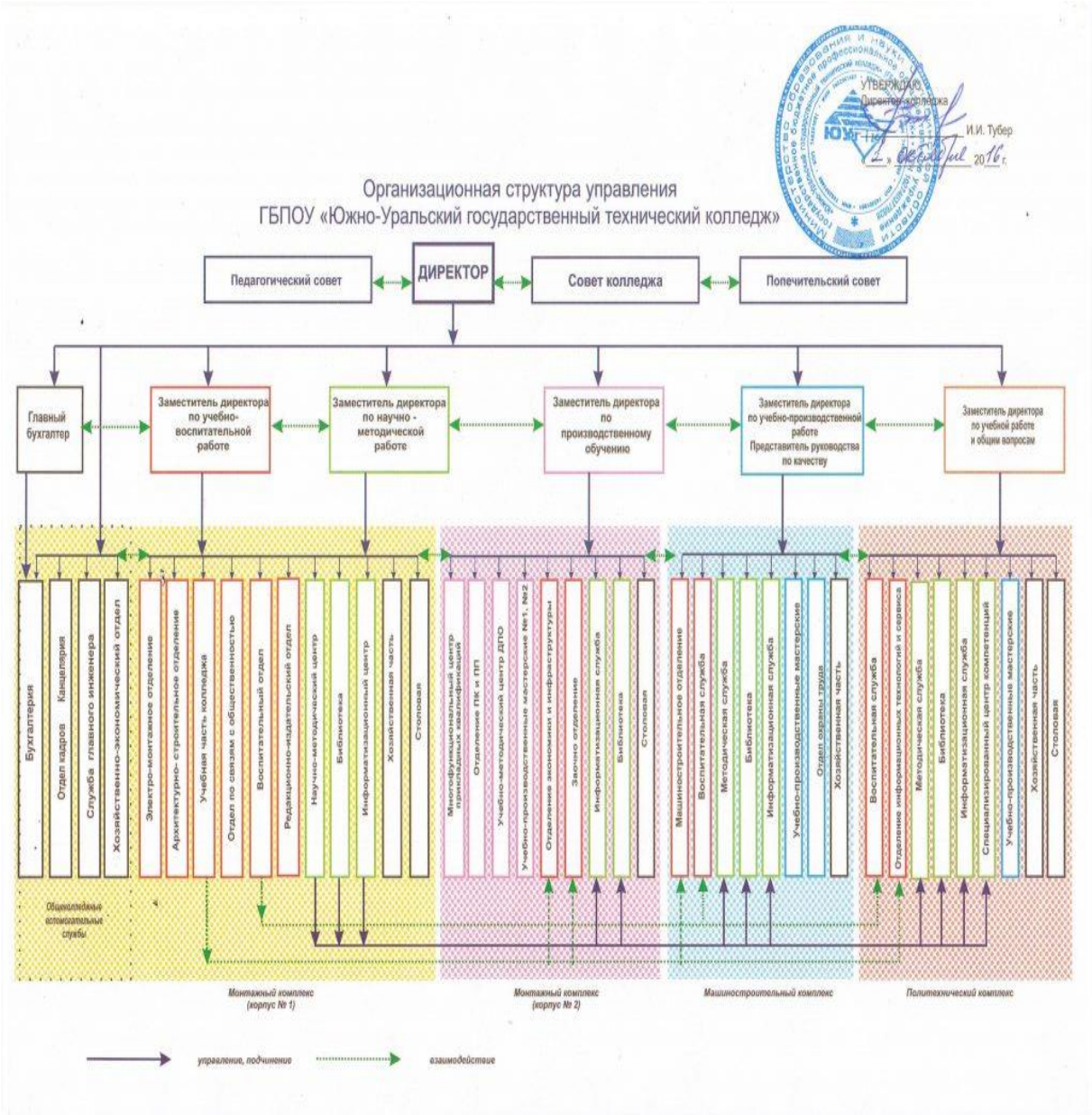

Рисунок 1 – Структура Южно-Уральского государственного технического колледжа на сегодняшний день

1.2 Расположение Южно-Уральского государственного технического колледжа

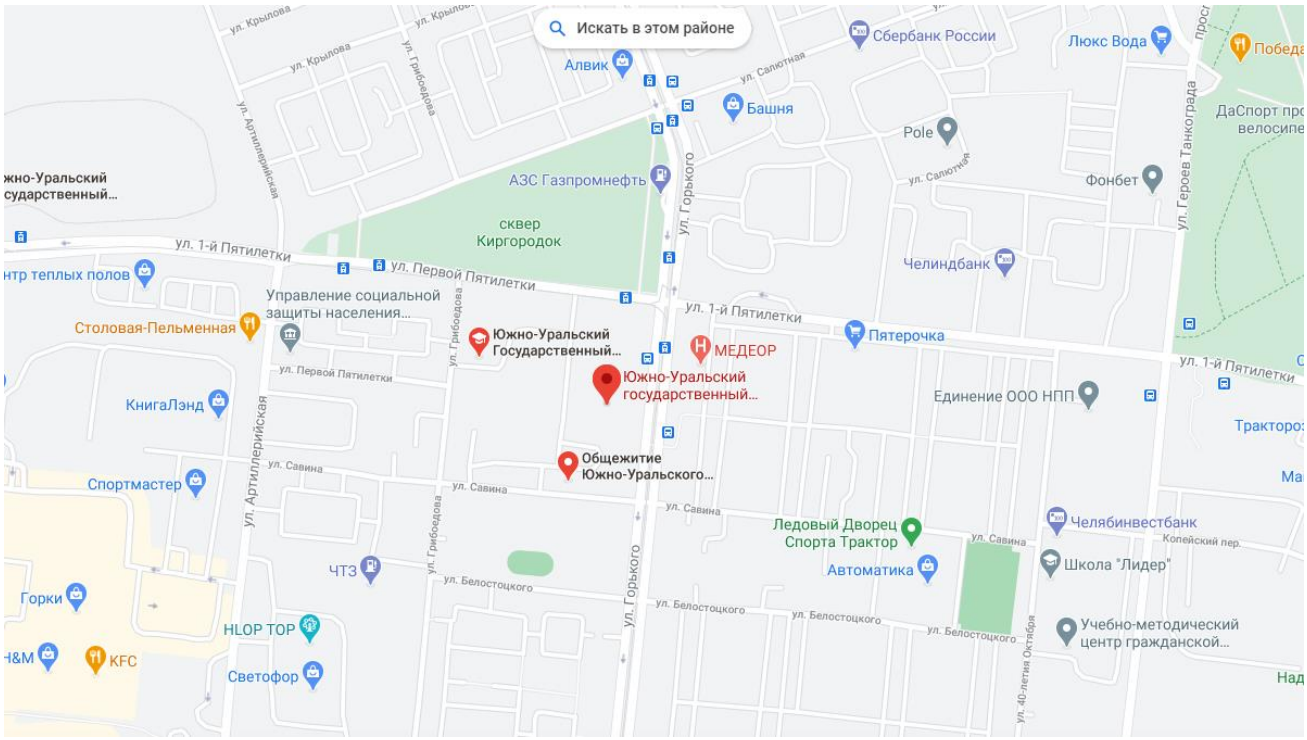

Рисунок 2 – Расположение Южно-Уральского государственного технического колледжа

1.3 Информационные технологии, используемые в организации

Используемое оборудование и программное обеспечение

Все сотрудники компании используют собственные ноутбуки, поэтому оборудование в компании включает два сервера с четырех ядерными процессорами INTEL Xeon E550. На обоих серверах установлена операционная система Windows 2016 Server, 32 ГБ оперативной памяти DDR3. Каждый из этих серверов включает два жестких диска размером 2 ТБ 7200 об / мин. На данных серверах расположены общие папки, настроенные по протоколу SMBv1. В данных папках у каждого сотрудника имеется своя личная папка куда и сохраняется вся резервная копия данных.

Так же в рамках моего анализа было обнаружено, что на данных папках не настроены разграничения прав доступа между преподавателями, что является очень важным фактором, так как разработка методического материала и любых программ для ЭВМ является объектами авторского права.

1.4 Планируемые изменения

Текущая система кажется слишком медленной и не надежной для компании и сотрудников, поэтому было бы целесообразно внести ряд изменений.

Здесь возможность использовать облачный FTP-сервер от https://lancloud.ru, и отказаться от хранения и обслуживания столь дорогих серверов.

Cloud Backup (BaaS) – это облачный сервис резервного копирования данных на базе одного из лидирующих на рынке решений - Veeam Backup & Replication с технологией Cloud Connect. Сервис позволяет выполнять резервное копирование любых физических или виртуальных серверов и рабочих станций и сохранять резервные копии в облаке LanCloud. Бэкапы будут размещены за пределами вашего офиса в надёжном ЦОД, сертифицированном по TIER-III Facility & Operation. Встроенная функция шифрования резервных копий на стороне клиента, позволяет быть на 100% уверенным в конфиденциальности передаваемой в облако информации.

1.5 Cloud Backup:

- Резервное копирование клиентских рабочих станций под управлением Windows или Linux с возможностью полного восстановления на другое железо или в виртуальную среду.

- Резервное копирование любых виртуальных серверов Hyper-V или VMware с возможностью полного восстановления состояния виртуальной машины или отдельных файлов

- Гранулярное восстановление приложений: Active Directory, Exchange, SharePoint, SQL Server и Oracle с возможностью восстановления отдельных объектов и баз данных

- Возможность шифрования данных на стороне клиента до передачи в облако

- Хранение резервных копий за пределами офиса в надёжном ЦОД TIER-III Facility & Operation.

- Возможность восстановление резервных копий в облако LanCloud в случае полного отказа локальной инфраструктуры

- Одна из самых выгодных цен на рынке за объём данных - 1 руб./мес. за 1 ГБ

Архивная резервная копия на текущем сервере, должна быть пересена на новый облачный сервер. Доступ к данным должен быть открыт для соответствующих пользователей, с разграничением прав доступа.

Решение этого вопроса будет частью практической части данной работы.

ГЛАВА 2. ТЕОРЕТИЧЕСКАЯ ОСНОВА РАБОТЫ

2.1 Резервное копирование

Резервное копирование - это механизм, в котором выбираются данные (могут быть не все)которые будут хранится на другом носителе. Если исходный носитель уничтожен, данные восстанавливаются с резервного носителя. Из вышесказанного следует, что при любом восстановлении мы всегда теряем какие-то данные. Как минимум те, которые были созданы после последней резервной копии. Цель состоит в том, чтобы выполнять резервное копирование как можно чаще, и делать это регулярно.

Резервное копирование - это процесс создания когерентной (непротиворечивой) копии данных. Подсистема резервного копирования - очень важная часть любой информационной системы. При правильной ее организации она способна решить сразу же две задачи. Во-первых, надежно защитить весь спектр важных данных от утери. Во-вторых, организовать быструю миграцию с одного ПК на другой в случае необходимости, то есть, фактически обеспечить бесперебойную работу офисных сотрудников. Только в этом случае можно говорить об эффективной работе резервного копирования. Овладение тактикой резервного копирования - неотъемлемый атрибут профессионализма пользователя и системного администратора. Вытекает она из решения пользователем для себя, какими методами и на каком уровне будет сохраняться информация (от этого зависит требуемое программное и аппаратное обеспечение), объема необходимой к сохранению информации (от этого зависят выбираемые информационные носители), размера и структуры локальной сети (от этого зависит реальный механизм систематического выполнения копирования).

Для выполнения процедуры резервного копирования обычно создаются специальные программно-аппаратные подсистемы, называемые подсистемами резервного копирования. Они как раз и предназначены как для проведения регулярного автоматического копирования системных и пользовательских данных, так и для оперативного восстановления данных. Хранение информации отдельно от системных файлов уже является обязательным правилом. В случае обычного пользователя это означает, как минимум, разделение HDD на три логических диска: для системы, для приложений, для данных. В случае корпоративного сотрудника с большим объемом конфиденциальной информации - размещение информации на других, не системных физических дисках. Эта мера облегчает и саму операцию архивирования данных. Принцип раздельного хранения информации относится и к файловым архивам и к образам дисков. Их необходимо также хранить как минимум на несистемных разделах одного HDD. В случае корпоративного пользователя принцип раздельного хранения информации должен реализовываться еще жестче: как минимум одна из копий должна храниться в отдельном месте, чтобы не потерять корпоративную информацию в случае непредвиденных обстоятельств.

2.2 Технологии резервного копирования

Обзор технологий резервного копирования

В зависимости от важности, хранимой на компьютере информации и от частоты её использования, выполняют несколько видов резервного копирования данных:

- Полное резервное копирование (Full backup).
- Дифференциальное резервное копирование (Differential backup).
- Инкрементное резервное копирование (Incremental backup).

Полное резервное копирование

Является главным и основополагающим методом создания резервных копий, при котором выбранный массив данных копируется целиком. Это наиболее полный и надежный вид резервного копирования, хотя и самый затратный. В случае необходимости сохранить несколько копий данных общий хранимый объем будет увеличиваться пропорционально их количеству. Для предотвращения большого объёма использованных ресурсов используют алгоритмы сжатия, а также сочетание этого метода с другими видами резервного копирования: инкрементным или дифференциальным. И, конечно, полное резервное копирование незаменимо в случае, когда нужно подготовить резервную копию для быстрого восстановления системы с нуля.

Достоинства метода:

Легкий поиск файлов - Поскольку выполняется резервное копирование всех данных, содержащихся на устройстве, для поиска нужного файла не требуется просматривать несколько носителей.

Текущая резервная копия всей системы всегда расположена на одном носителе или наборе носителей - Если потребуется восстановить всю систему, то всю необходимую информацию можно найти в последней полной резервной копии.

Недостатки метода:

Избыточная защита данных - поскольку большинство файлов системы изменяются достаточно редко, то каждая последующая полная резервная копия представляет собой копию данных, сохраненных в ходе первого полного резервного копирования. Для полного резервного копирования требуется большой объём носителя.

Полное резервное копирование занимает больше времени - Для создания полных резервных копий может потребоваться длительное время, в особенности, если для хранения выбраны устройства в сети.

Дифференциальное резервное копирование

Отличается от инкрементного тем, что копируются данные с последнего момента выполнения Full backup. Данные при этом помещаются в архив «нарастающим итогом». В системах семейства Windows этот эффект достигается тем, что архивный бит при дифференциальном копировании не сбрасывается, поэтому измененные данные попадают в архивную копию, пока полное копирование не обнулит архивные биты.В силу того, что каждая новая копия, созданная таким образом, содержит данные из предыдущей, это более удобно для полного восстановления данных на момент аварии. Для этого нужны только две копии: полная и последняя из дифференциальных, поэтому вернуть к жизни данные можно гораздо быстрее, чем поэтапно накатывать все инкременты. К тому же этот вид копирования избавлен от вышеперечисленных особенностей инкрементного, когда при полном восстановлении старые файлы, возрождаются из пепла. Возникает меньше путаницы. Но дифференциальное копирование значительно проигрывает инкрементному в экономии требуемого пространства. Так как в каждой новой копии хранятся данные из предыдущих, суммарный объем зарезервированных данных может быть сопоставим с полным копированием. И, конечно, при планировании расписания (и расчетах, поместится ли процесс бэкапа во временное «окно») нужно учитывать время на создание последней, самой большой, дифференциальной копии.

Достоинства метода:

Легкий поиск файлов - Для восстановления системы, защищенной с помощью стратегии дифференциального резервного копирования требуются две резервные копии - последняя полная резервная копия и последняя дифференциальная резервная копия. Время восстановления значительно меньше по сравнению со стратегиями резервного копирования, для которых требуются последняя полная резервная копия и

все инкрементальные резервные копии, созданные с момента последнего полного резервного копирования.

Меньшее время резервного копирования и восстановления - Дифференциальное резервное копирование занимает меньше времени, чем полное резервное копирование. Восстановление после аварии выполняется быстрее, поскольку для полного восстановления устройства необходимы только последняя полная резервная копия и дифференциальная резервная копия.

Недостаток метода:

Избыточная защита данных - Сохраняются все файлы, измененные с момента последнего инкрементального резервного копирования. Таким образом, создаются избыточные резервные копии.

Инкрементное резервное копирование

В отличие от полного резервного копирования в этом случае копируются не все данные (файлы, сектора и т.д.), а только те, что были изменены с момента последнего копирования. Для выяснения времени копирования могут применяться различные методы, например, в системах под управлением операционных систем семейства Windows используется соответствующий атрибут файла (архивный бит), который устанавливается, когда файл был изменен, и сбрасывается программой резервного копирования. В других системах может использоваться дата изменения файла. Понятно, что схема с применением данного вида резервного копирования будет неполноценной, если время от времени не проводить полное резервное копирование. При полном восстановлении системы нужно провести восстановление из последней копии, созданной Full backup, а потом поочередно восстановить данные из инкрементных копий в порядке их создания. Данный вид используется для того, чтобы в случае создания архивных копий сократить расходуемые объемы на устройствах хранения информации (например, сократить число

используемых ленточных носителей). Также это позволит минимизировать время выполнения заданий резервного копирования, что может быть крайне важно в условиях, когда машина работает постоянно, или прокачивать большие объемы информации. У инкрементного копирования есть один нюанс: поэтапное восстановление возвращает и нужные удаленные файлы за период восстановления. Например: допустим, по выходным дням выполняется полное копирование, а по будням инкрементное. Пользователь в понедельник создал файл, во вторник его изменил, в среду переименовал, в четверг удалил. Так вот при последовательном поэтапном восстановлении данных за недельный период мы получим два файла: со старым именем за вторник до переименования, и с новым именем, созданным в среду. Это произошло потому, что в разных инкрементных копиях хранились разные версии одного и того же файла, и в итоге будут восстановлены все варианты. Поэтому при последовательном восстановлении данных из архива «как есть» имеет смысл резервировать больше дискового пространства, чтобы смогли поместиться в том числе и удаленные файлы.

Достоинства метода:

Эффективное использование носителей - Поскольку сохраняются только файлы, измененные с момента последнего полного или инкрементального резервного копирования, резервные копии занимают меньше места.

Меньшее время резервного копирования и восстановления - Инкрементальное резервное копирование занимает меньше времени, чем полное и дифференциальное резервное копирование.

Недостаток метода:

Данные резервного копирования сохраняются на нескольких носителях - Поскольку резервные копии расположены на нескольких носителях, восстановление устройства после аварии может занять больше

времени. Кроме того, для эффективного восстановления работоспособности системы носители должны обрабатываться в правильном порядке.

2.3 Технологии хранения резервных копий и данных

В процессе выполнения резервного копирования данных появляется проблема выбора технологии хранения резервных копий и данных. В настоящее время особой популярностью пользуются следующие виды носителей:

- Накопители на магнитных лентах.
- Дисковые накопители.
- Сетевые технологии.
- Облачные технологии

Накопители на магнитных лентах.

Накопители на магнитной ленте применяются вместе с компьютерами еще с начала 50-х годов - именно тогда они стали приходить на смену «бумажным» носителям информации - перфолентам и перфокартам. Немаловажный фактор, обеспечивающий столь продолжительный интерес к накопителям на магнитной ленте, - низкая стоимость хранения информации. Основная проблема при использовании накопителей на магнитной ленте сегодня заключается в том, что множество таких устройств использует несовместимые друг с другом форматы записи данных на магнитной ленте. Это часто затрудняет не только выбор конкретного накопителя, но и обмен данными при его эксплуатации.

Дисковые накопители.

Существует два наиболее часто встречающихся вида дисковых накопителей: накопители на жёстких магнитных дисках и накопители на оптических дисках.

Накопители на жестких магнитных дисках (Hard Disk Drive, HDD) являются основными устройствами оперативного хранения информации. Для современных одиночных накопителей характерны объемы от сотен мегабайт до нескольких гигабайт при времени доступа 5-15 мс и скорости передачи данных 1-10 Мбайт/с. Относительно корпуса сервера различают внутренние и внешние накопители. Внутренние накопители существенно дешевле, но их максимальное количество ограничивается числом свободных отсеков корпуса, мощностью и количеством соответствующих разъемов блока питания сервера. Установка и замена обычных внутренних накопителей требует выключения сервера, что в некоторых случаях недопустимо. Внутренние накопители с возможностью "горячей" замены (Hot Swap) представляют собой обычные винчестеры, установленные в специальные кассеты с разъемами. Кассеты обычно вставляются в специальные отсеки со стороны лицевой панели корпуса, конструкция позволяет вынимать и вставлять дисководы при включенном питании сервера. Для стандартных корпусов существуют недорогие приспособления (Mobile Rack), обеспечивающие оперативную съемность стандартных винчестеров. Внешние накопители имеют собственные корпуса и блоки питания, их максимальное количество определяется возможностями интерфейса. Обслуживание внешних накопителей может производиться и при работающем сервере, хотя может требовать прекращения доступа к части дисков сервера.

Для больших объемов хранимых данных применяются блоки внешних накопителей - дисковые массивы и стойки, представляющие собой сложные устройства с собственными интеллектуальными контроллерами, обеспечивающими, кроме обычных режимов работы, диагностику и тестирование своих накопителей. Более сложными и надежными устройствами хранения являются RAID-массивы (Redundant Array of Inexpensive Disks - избыточный массив недорогих дисков). Для

пользователя RAID представляет собой один (обычно SCSI) диск, в котором производится одновременная распределенная избыточная запись (считывание) данных на несколько физических накопителей (типично 4-5) по правилам, определяемым уровнем реализации (0-10). Например, RAID Level 5 позволяет при считывании исправлять ошибки и осуществлять замену любого диска без остановки обращения к данным.

Устройства считывания компакт-дисков CD-ROM расширяют возможности системы хранения данных NetWare. Существующие накопители обеспечивают скорость считывания от 150 кбайт/с до 300/600/900/1500 Кбайт/с для 2-,4-,6- и 10-скоростных моделей при времени доступа 200-500 мс. NetWare позволяет монтировать компакт-диск как сетевой том, доступный пользователям для чтения. Объем тома может достигать 682 Мбайт (780 Мбайт для Mode 2). Устройства CD-ROM выпускаются с различными интерфейсами, как специфическими (Sony, Panasonic, Mitsumi), так и общего применения: IDE и SCSI. Сервер NetWare обслуживает только CD-ROM с интерфейсами SCSI, новые драйверы существуют и для IDE; устройства со специфическими интерфейсами могут использоваться только в DOS для инсталляции системы. С точки зрения повышения производительности предпочтительнее использование CD-ROM SCSI, однако они существенно дороже аналогичных IDE-устройств. В сервере с дисками SCSI применение CD-ROM с интерфейсом IDE может оказаться невозможным из-за конфликтов адаптеров.

Достоинствами таких накопителей является:

- быстрый доступ к данным.

- возможность параллельного доступа к данным без значительной потери скорости.

Недостатки дисковых накопителей:

- более высокая стоимость чем ленты.

- более высокое энергопотребление.

- более дорогое расширение системы хранения данных.

- невозможность обеспечения высокой безопасности копий .

Сетевые технологии

Сетевое хранение данных построено на трех фундаментальных компонентах: коммутации, хранении и файлах. Все продукты хранения можно представить в виде комбинации функций данных компонентов. Поначалу это может вызвать замешательство: поскольку продукты хранения разрабатывались по совершенно разным направлениям, функции часто перекрывают друг друга.

В сети работает множество приложений типа «клиент-сервер» и различных видов распределенных приложений, но в то же время хранение является уникальным и специализированным типом приложения, которое может функционировать в нескольких сетевых средах. Поскольку процессы хранения тесно интегрированы с сетями, будет уместно напомнить, что сетевые хранилища представляют собой системные приложения. Сервисами, которые предоставляются сетевыми приложениями хранения, могут пользоваться сложные корпоративные программы и пользовательские приложения. Как и в случае со многими технологиями, некоторые типы систем лучше отвечают требованиям сложных приложений высокого уровня.

Термин «коммутация» применяется ко всему программному и аппаратному обеспечению и к службам, которые обеспечивают транспортировку хранения и управление ею в сетевом хранилище. Сюда входят такие различные элементы, как разводка кабелей, сетевые контроллеры ввода-вывода, коммутаторы, концентраторы, аппаратура выборки адресов, контроль связи данных, транспортные протоколы, безопасность и резервы ресурсов. В сетевых хранилищах все еще широко используются технологии шин данных SCSI и ATA, и, скорее всего, они

будут использоваться еще долго. Фактически продукты SCSI и ATA сегодня применяются гораздо чаще в технологии NAS.Существуют два важных различия между сетями хранения SAN и обычными локальными сетями LAN. Сети хранения SAN автоматически синхронизируют данные между отдельными системами и хранилищами. В сетевых хранилищах необходимы компоненты высокой степени точности для обеспечения надежной и предсказуемой среды. Несмотря на ограничения по расстоянию, параллельная SCSI - чрезвычайно надежная и предсказуемая технология. Если новые технологии коммутации, такие как Fibre Channel, Ethernet и InfiniBand, сменят SCSI, они должны будут продемонстрировать аналогичный или лучший уровень надежности и предсказуемости. Имеется и такая точка зрения, которая рассматривает коммутацию как канал хранилища. Сам термин «канал», берущий свое начало в среде больших вычислительных машин, предполагает высокую надежность и работоспособность.

Хранение в основном затрагивает блочные операции адресного пространства, включая создание виртуальной среды, когда адреса логического блока хранения отображаются из одного адресного пространства в другое. Вообще говоря, в сетевых хранилищах функция хранения почти не изменилась, если не считать двух заметных отличий. Первое - это возможность нахождения технологий виртуализации устройства, например управление устройством внутри оборудования сетевого хранения. Этот вид функции иногда называют контроллером домена хранения или виртуализацией LUN. Второе главное отличие хранения заключается в масштабируемости. Продукты хранения, такие как подсистемы хранения, имеют значительно больше контроллеров/интерфейсов, чем предыдущие поколения шинной технологии, а также намного больший объем хранения.

Функция организации файлов представляет абстрактный объект конечному пользователю и приложениям, а также организует разметку данных на реальных или виртуальных устройствах хранения. Основную часть функциональности файлов в сетевых хранилищах обеспечивают файловые системы и базы данных; их дополняют приложения управления хранением, например операции резервного копирования, также являющиеся файловыми приложениями. Сетевое хранение к настоящему времени почти не изменило файловые функции, за исключением разработки файловых систем NAS, в частности файловой системы WAFL компании Network Appliance. Кроме упомянутых технологий хранения данных NAS и SAN, ориентированных на крупные и глобальные сети, в небольших локальных сетях доминирующее положение занимает технология DAS, в соответствии с которой хранилище находится внутри сервера, обеспечивающего объем хранилища и необходимую вычислительную мощность.

Простейшим примером DAS может служить накопитель на жестком диске внутри персонального компьютера или ленточный накопитель, подключенный к единственному серверу. Запросы ввода-вывода (называемые также командами или протоколами передачи данных) непосредственно обращаются к этим устройствам. Однако такие системы плохо масштабируются, и компании с целью расширения объема хранилища вынуждены приобретать дополнительные серверы. Эта архитектура очень дорогая и может использоваться только для создания небольших по объему хранилищ данных.

Онлайн-сервис резервного копирования

Широкополосный доступ в Интернет стал стандартом, что привело к появлению онлайн-резервного копирования. Онлайн сервисы - их популярность растет: не нужно беспокоиться о безопасности данных, они также доступны немедленно и прежде всего из любого места. Кроме того,

он прост в использовании и не требует специальных технических средств. Скорость восстановления ограничена скоростью соединения (что является проблемой только для действительно больших объемов данных). Недостатки: если мы не «видим» вопрос безопасности данных, мы практически не будем на него влиять. Необходимо обеспечить безопасность при передаче данных в сервис резервного копирования. Типичным примером службы резервного копирования в Интернете является DropBox. DropBox - это сервис, позволяет синхронизировать файлы между несколькими компьютерами. Вам необходимо установить его, чтобы использовать программное обеспечение, которое поддерживает синхронизацию одного каталога (даже с подкаталогами) на вашем диске против сервера. Таким образом, может быть подключено больше компьютеров, и во всех каталогах те же данные. После отключения от интернета можно работать с данными локально, но синхронизация с сервером будет производиться снова только после подключения к Интернету. DropBox также может поддерживать несколько версий файлы, поэтому вы можете легко восстановить старую версию файла с сервера. Клиент DropBox существует для Linux, MS Windows и Mac OS, а также есть возможность управления через веб интерфейс. Эта услуга доступна бесплатно в базовой форме

2.4 Протоколы передачи данных на удаленный сервер

Протокол передачи файлов (FTP)

Очень часто используемым средством удаленного резервного копирования является FTP-сервер. Как имя предполагает, что данные передаются на этот сервер через FTP. Этот Протокол работает на прикладном уровне TCP / IP, использует протокол TCP для передачи данных и является независимая платформа. Данные могут передаваться как в текстовом, так и в двоичном формате. 26 Протокол FTP работает по

классической модели клиент-сервер, которая основана на том, что клиентский компьютер отправляет запросы на сервер, а затем сервер их обрабатывает. Есть два способа работы с FTP, которые мы называем активным и пассивным режимом.

Активный режим

1. Клиент подключается к серверу через порт 21.

2. Клиент отправляет на сервер информацию о выбранном порте на своей стороне.

3. Клиент начинает прослушивание выбранного порта.

4. Сервер подключается к порту через свой порт ftp-data.

5. Передача данных будет происходить по текущему открытому каналу.

6. Отправляющая сторона закрывает порт, указывая на окончание соединения.

Пассивный режим

1. Клиент подключается к серверу через порт 21 и запрашивает переход в пассивный режим.

2. Сервер отправляет клиенту информацию о выбранном порте на своей стороне.

3. Сервер начинает прослушивание выбранного порта.

4. Клиент подключается к выбранному порту со своего порта.

5. Передача данных будет происходить по текущему открытому каналу.

6. Сторона, отправившая данные, закрывает порт, указывая на окончание соединения.

Secure Shell (SSH)

SSH обеспечивает безопасную альтернативу традиционным протоколам для удаленных сеансов и передача файлов, например Telnet. Этот протокол поддерживает удаленную аутентификацию, тем самым

сводя к минимуму угрозу спуфинга клиента путем подмены IP-адреса или Манипуляции с DNS. SSH поддерживает широкий спектр алгоритмов шифрования секретных ключей. (DES, 3DES, IDEA и BlowFish) (6).

SSH работает следующим образом:

1. Клиент использует локальный порт с большим номером и подключается к порту 22 сервера.

2. Клиент и сервер договариваются о версии SSH, которую они будут использовать.

3. Клиент запрашивает открытый ключ и ключ хоста.

4. Клиент и сервер соглашаются использовать алгоритм шифрования.

5. Клиент генерирует сеансовый ключ и шифрует его, используя открытый ключ сервера.

6. Сервер шифрует сеансовый ключ, повторно шифрует его, используя открытый ключ клиента, и отправляет обратно клиенту для проверки.

7. Пользователь аутентифицируется на сервере в потоке данных, зашифрованном с помощью ключа. сеанс.

8. Соединение установлено, и на сервере может выполняться интерактивная работа

Системы контроля версий

Управление версиями - это метод, который позволяет вам вести историю всех внесенных вами изменений.

Это позволяет пользователю в любой момент вернуться к более старой версии файла, если ошибки возникают во время работы. Управление версиями чаще всего используется в случае исходных кодов.

Для управления версиями используются разные системы управления версиями, самые известные из них перечислены ниже.

Система одновременных версий (CVS)

Эта система очень популярна среди разработчиков. Первоначально CVS предотвращала разногласия между версией, над которыми работают отдельные разработчики, разрешая редактировать только самые последние версии кода,а другие версии заблокированы от таких изменений. Теперь это позволяетразделить проект на разные ветки, чтобы разработчики могли вносить измененияне зависимо от других, а затем объединить эти ветви в конечный продукт.

CVSработает в системах Unix через клиентское программное обеспечение, которое можно запускатьв нескольких операционных системах. Считается одной из самых передовых систем управления.

Преимущества CVS:

- Она используется много лет и считается очень продвинутой системой

Недостатки CVS:

- Обновление не записывается при переименовании или перемещении файла;
- Угрозы безопасности при использовании символьных файловых ссылок;
- Не поддерживает атомарные операции

Appache Subversion (SVN)

Система SVN создавалась как альтернатива CVS, которая должна была исправить некоторые недостатки CVS и в то же время поддерживать высокую совместимость с CVS. SVN доступен так же, как CVS бесплатно и является программным обеспечением с открытым исходным кодом, выпущенным под лицензией Apache. SVN, в отличие от CVS поддерживает выполнение атомарных операций. Либо все изменения записываются в исходном файле либо нет, что означает отсутствие частичных изменений нарушающих исходный файл.

Многие разработчики перешли на использование SVN, потому что это более новая технология, берущая лучшее из CVS и еще больше расширяющая эти возможности.

Преимущества SVN:

-Это более современная система, основанная на CVS;

-Поддерживает выполнение атомарных операций;

-Менее требовательные операции при разветвлении проектов;

-Широкий набор плагинов IDE.

Недостатки SVN:

-Он по-прежнему содержит ошибки, связанные с переименованием файлов и каталогов;

-Отсутствие команд для управления репозиторием;

-Медленнее по сравнению с CVS (16)

Git

Git использует контроль версий с совершенно иной точки зрения, чем CVS и SVN. Оригинальная идея заключалась в том, чтобы создать более быструю распределенную систему контроля версий, которая была бы открытой и противоречила обычаям и практике, которые мы знаем из CVS. Эта система в первую очередь предназначенадля Linux и на этой платформе он также самый быстрый. Он не очень подходит для независимых разработчиков или для небольших команд разработчиков, потому чтофайлы могут быть недоступны, если пользователь не использует компьютер с репозиторием.

Преимущества Git:

- Подходит для пользователей, которым не нравятся системы CVS и SVN;

- Значительно более быстрое выполнение операций;

- Менее требовательные операции при ветвлении проекта;

- Полная запись истории также доступна при работе в автономном режиме

Недостатки Git:

- Пользователям SVN может быть сложнее привыкнуть к Git;
- Не подходит для автономных разработчиков;
- Ограниченная поддержка Windows

2.5 Технология RAID

RAID (избыточный массив недорогих / независимых дисков) - это технология используемая для защиты данных в случае отказа диска. Эта технология имеет несколько уровней, из которых каждый защищает данные по-разному.

RAID может быть реализован с помощью аппаратного или программного обеспечения, либо их комбинации. Аппаратный RAID обычно проще в использовании, потому что он предоставляет его сразу после запуска аппаратного устройства.

Программный RAID использует программное обеспечение, что означает нагрузку на процессор.

RAID 0

RAID 0 - это просто комбинация нескольких дисков в один блок. Фактически эта технология служит только для увеличения производительности дисководов, при этом вероятность выхода из строя увеличивается, потому что есть больше юнитов, которые могут выйти из строя и сделать недоступными определенную часть данных. Для реализации RAID 0 требуется минимум два диска. Лучшая производительность достигается, когда у каждого устройства есть собственный контроллер, даже если в этом нет необходимости.

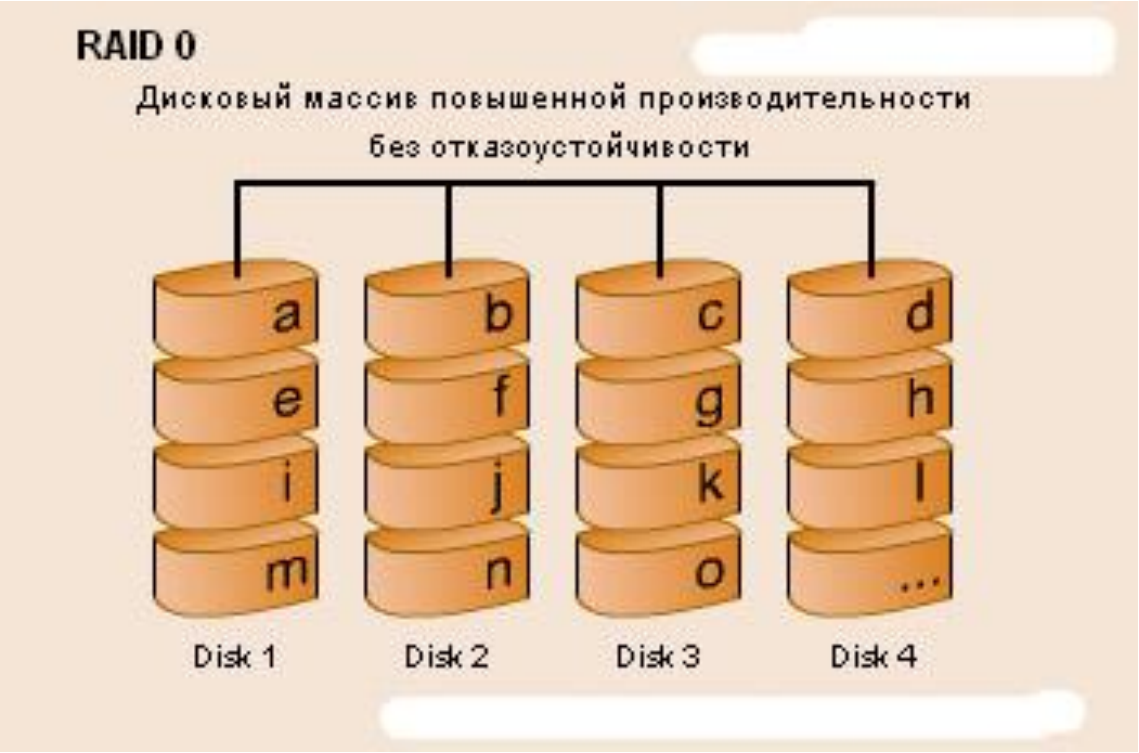

Рисунок 3 – RAID 0

RAID 1

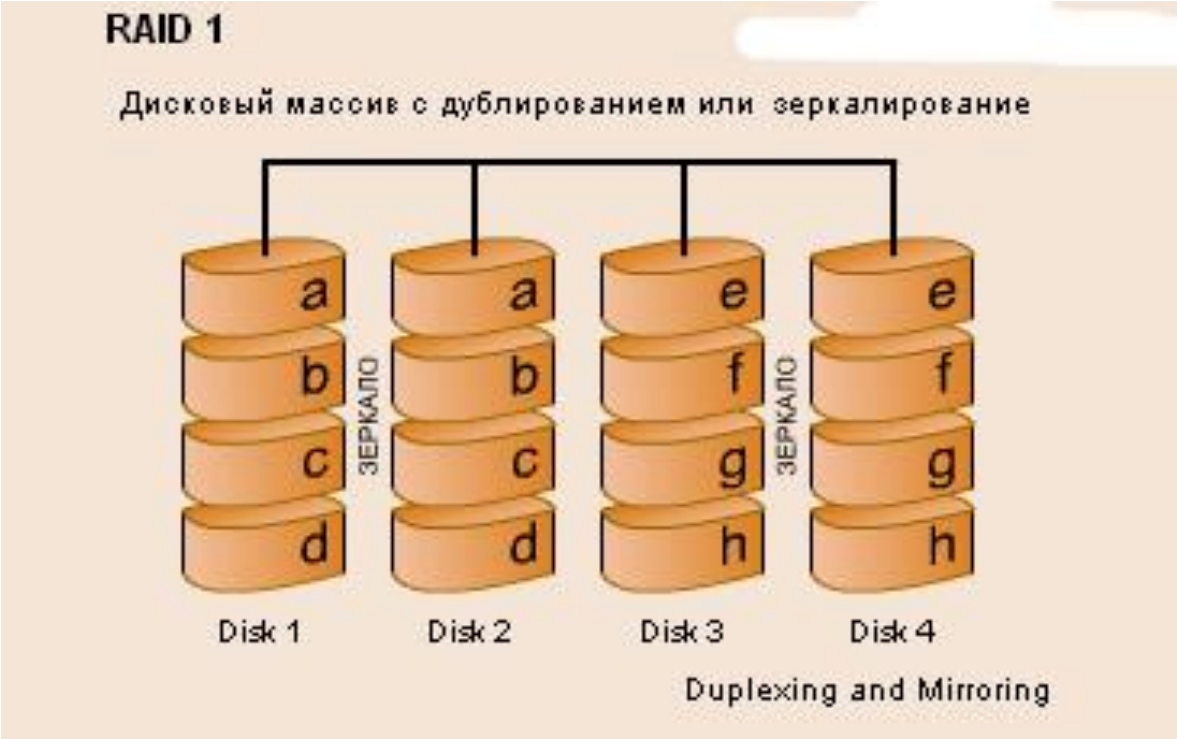

Рисунок 4 – RAID 1

RAID 1, часто также называемый зеркалированием, повторяет запись с одного диска на другой диск. Это увеличивает отказоустойчивость, так как под рукой есть текущая резервная копия. Выход из строя одного из дисков, что является одним из наиболее частых отказов оборудования RAID 1, не является критичной проблемой, так как достаточно заменить поврежденный диск и диски снова синхронизируются. Скорость записи здесь слабее, потому что данные записываются в большее количество секторов одновременно.Для реализации RAID 1 требуется минимум два диска.

RAID 2

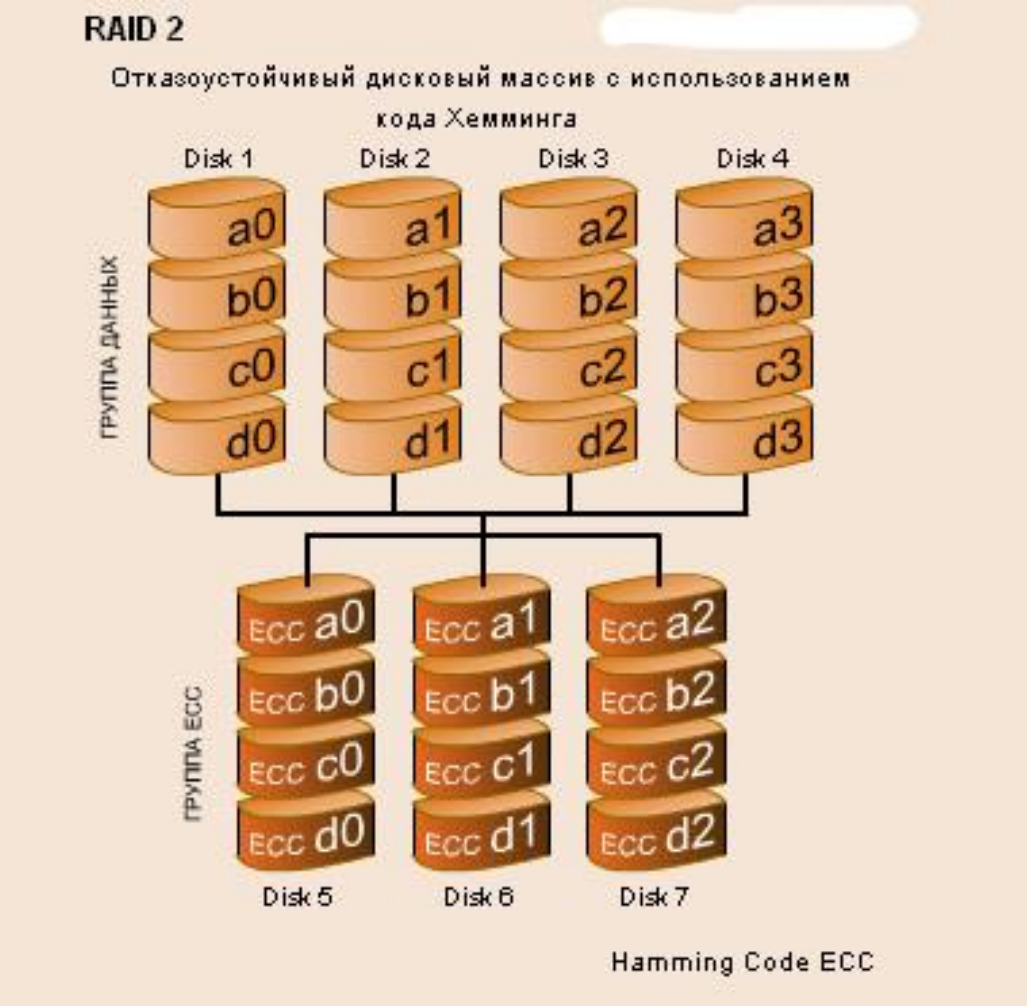

Рисунок 5 – RAID 2

RAID 2 - Отказоустойчивый дисковый массив с использованием кода Хемминга Hamming Code ECC

RAID 2 - использует коды исправления ошибок Хемминга (Hamming Code ECC). Коды позволяют исправлять одиночные и обнаруживать двойные неисправности.

Преимущества:

- быстрая коррекция ошибок ("на лету");

- очень высокая скорость передачи данных больших объемов;

- при увеличении количества дисков, накладные расходы уменьшаются;

- достаточно простая реализация

Недостатки:

- высокая стоимость при малом количестве дисков;

- низкая скорость обработки запросов (не подходит для систем ориентированных на обработку транзакций)

RAID 3

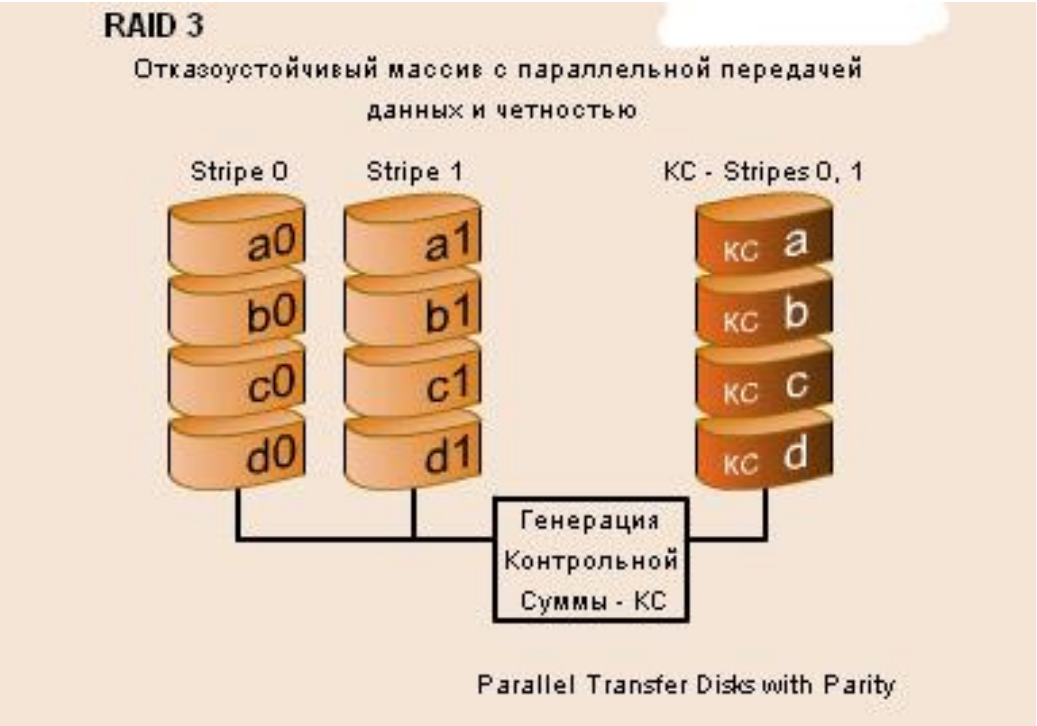

Рисунок 6 – RAID 3

Отказоустойчивый массив с параллельной передачей данных и четностью Parallel Transfer Disks with Parity

RAID 3 - данные хранятся по принципу striping на уровне байтов с контрольной суммой на одном из дисков. Массив не имеет проблему некоторой избыточности как в RAID 2-го уровня. Диски с контрольной суммой используемые в RAID 2, необходимы для определения ошибочного заряда. Однако большинство современных контроллеров способны определить, когда диск отказал при помощи спец сигналов или дополнительного кодирования информации, записанной на диск и используемой для исправления случайных сбоев.

Преимущества:

- очень высокая скорость передачи данных;

- отказ диска мало влияет на скорость работы массива;

- малые накладные расходы для реализации избыточности.

Недостатки:

-непростаяреализация;

-низкая производительность при большой интенсивности запросов данных небольшого объема.

RAID 4

RAID 4 - это решение, очень похожее на RAID 3. Он отличается от RAID 3 тем, что читает на уровне блока вместо байтов. Показания менее одного блока обычно очень быстрые и обычно эта скорость увеличивается с каждой добавленной единицей. Для реализации RAID 4, как и в случае с RAID 3, требуется минимум три диска.

RAID 5

RAID 5 похож на RAID 4. Он также позволяет разбивать на разделы и записывать данные для исправления ошибок, которые приводят к повышению производительности и отказоустойчивости. Данные о четности хранятся на каждом блоке. Скорость записи выше, чем у RAID 4, а скорость чтения наоборот медленнее, потому что информация о четности

занимает место на каждом блоке, и эти данные необходимо пропускать при чтении.

RAID 5 очень подходит для серверов баз данных. Для реализации RAID 5 требуется минимум три диска

RAID 10

RAID 10 представляет собой комбинацию RAID 1 и RAID 0. Он предлагает все преимущества в производительности разделения и также повысить отказоустойчивость за счет зеркалирования. Минус здесь - более высокая цена, поскольку реализация этого варианта требует использования как минимум четырех дисков. RAID 10 подходит для серверов баз данных, поскольку обеспечивает высокую производительность и отказоустойчивость.

RAID 0 + 1

Вариант RAID 0 + 1 часто путают с вариантом RAID 10. RAID 10 - это многораздельный массив. диски с зеркальными сегментами, где RAID 0 + 1 - зеркальный массив сегментированные единицы. Этот вариант подходит в ситуациях, когда больше делается упор на производительность, чем на надежность. Как и RAID 10, это решение относительно дорогое и для реализации требуется минимум четыре диска

Международный стандарт ISO/IEC 27001:2013

В этом подразделе я представляю цели мер, содержащихся в этом стандарте, разделенные на отдельные секторы информационной безопасности

Политика безопасности

Эта часть стандарта содержит требования к политике информационной безопасности. Цель - определить направление и экспресс-поддержка информационной безопасности со стороны руководства в соответствии с требованиями организации

2.6 Организация информационной безопасности

Целью является управление безопасностью информации в организации и поддержание информационной безопасности. организация и средства обработки информации, которая доступна, обрабатывается, передается или управляется внешними органами

Управление активами

Цель состоит в том, чтобы установить и поддерживать адекватную защиту активов организации и гарантировать, что информация получили адекватный уровень защиты

Безопасность человеческих ресурсов

Цель состоит в том, чтобы убедиться, что сотрудники, подрядчики и третьи стороны понимают свои обязанности и ответственность, чтобы быть в курсе угроз и проблем безопасности, связанных с ними.

Физическая и экологическая безопасность

Цель состоит в том, чтобы предотвратить несанкционированный физический доступ в зоны ограниченного доступа и к информации организации, чтобы предотвратить потерю, повреждение, кражу или компрометацию активов

Управление дорогами и управление движением

Целью является обеспечение правильной и безопасной работы средств обработки информации, создание и поддержкаадекватногоуровня информационной безопасности, минимизация риска сбоя системы,защита целостности программного обеспечения и данных, поддержка целостности и доступность информации и средства для их обработки, для обеспечения защиты информации в компьютерных сетях и защиты, поддерживающая инфраструктура, предотвращение несанкционированного раскрытия, модификации, потери или повреждение активов, обеспечение безопасности информации и программ при их обмене внутри организаций и при их обмене с внешними объектами

Приобретение, разработка и обслуживание информационных систем

Цель состоит в том, чтобы гарантировать, что безопасность станет неотъемлемой частью информационных систем, предотвращать ошибки, потерю, несанкционированное изменение или неправильное использование информации в приложениях, защищать конфиденциальность и целостность информации криптографическими средствами, обеспечивать безопасность системных файлов, обеспечение безопасности программного обеспечения и информация о прикладных системах, чтобы снизить риски, связанные с использованием опубликованных технические уязвимости

Управление инцидентами безопасности

Цель состоит в том, чтобы сообщать о событиях безопасности и уязвимостях информационной системы. таким образом, чтобы обеспечить своевременное начало корректирующих действий, обеспечить адекватные и эффективный подход к управлению инцидентами безопасности

Управление непрерывностью бизнеса

Цель состоит в том, чтобы предотвратить перебои в работе и защитить критически важные процессы организации от последствия серьезных сбоев информационных систем и обеспечение своевременного возобновления деятельности.

Соответствие требованиям

Цель состоит в том, чтобы избежать нарушений уголовного или гражданского права, правовых или статутных норм. договорные обязательства и требования безопасности.Убедитесь, что системы соответствуют требованиям с политиками и стандартами безопасности организации, максимизировать эффективность аудита; а также минимизировать вмешательство в информационные системы

План восстановления

План выхода из кризиса служит для поддержания непрерывности деятельности компании в случае серьезного сбой информационных технологий, ведущий к потере информации. Пусть будет эта неудача вызвано стихийным бедствием, человеческой ошибкой или целевой атакой на данные компании, всегда нужно минимизировать ущерб и как можно быстрее восстановить исходное состояние информации. Хотя не все инциденты можно предотвратить, их последствия всегда можно значительно уменьшить. через соответствующее планирование процедур в кризисных ситуациях. Ключ в том, чтобы всегда иметь хорошо продуманный план восстановления, применимый к текущей ситуации (8).

План восстановления должен включать следующее:

– Формирование команды антикризисного управления;

– Определение условий, при которых ситуация может быть классифицирована как нарушение безопасности;

– Способ начала восстановительных работ;

– Принципы коммуникации в антикризисном управлении;

– Спецификация основных процессов восстановительных работ;

– Выбор альтернативного рабочего места на время кризисной ситуации;

– Утверждение предупредительных мер;

– Документация плана восстановления;

– Способы обучения членов кризисной команды

ГЛАВА 3. ПРАКТИЧЕСКАЯ ЧАСТЬ

3.1 Предложение решения

В этой части работы я остановлюсь на конкретном предложении по решению обозначенной проблемы указанной в аналитической части.Я постараюсь улучшить и изменить существующую систему так, чтобы она была возможна для использования даже после внесения запланированных изменений.Наибольший упор будет сделан на надежность резервного копирования и сокращение времени, необходимого для его реализации.Поскольку это предлагаемое решение для относительно небольшой компании, учту его финансовую доступность.

Дизайн классификации данных

Данные компании будут разделены на категории, перечисленные в аналитической части работы следующим образом:

Публичная информация

Эта категория включает информацию, обычно доступную в Интернете или в прессе, в зависимости от ситуации. Сюда входит, в частности, следующая информация:

– Интернет-презентация;

– Статьи и публикации, публикуемые сотрудниками компании;

– Методические материалы разрабатываемые научными сотрудниками;

– Архив выпускных работ выпускников;

Внутренние данные

Сотрудники используют эти данные для выполнения своих должностных обязанностей и не могут использовать эти данные для предоставления третьей стороне. Эта информация не должна выходить за пределы компании. В этой категории я бы рекомендовал включить следующие данные:

– Электронная переписка со студентами и между отдельными сотрудниками;

– Отчеты о работе преподавателей;

– Краткосрочные стратегические планы компании;

– Контракты и счета-фактуры;

– Персональные данные сотрудников и клиентов. Секретные данные Доступ к этим данным имеют только уполномоченные лица в компании. Остальные сотрудники эти данные предоставляются только в исключительных случаях, например, если он сотрудник ему нужно делать свою работу.

Сюда входят следующие данные:

– Данные, относящиеся к интеллектуальной собственности студентов и сотрудников;

– Данные о студентах либо учениках (если компания с ними работает);

– Долгосрочные стратегические планы компании;

– Подробная информация о механизмах безопасности, используемых в компании.

3.2 Метод резервного копирования данных

Резервное копирование данных в зависимости от их классификации Способ резервного копирования данных будет зависеть от указанной выше классификации. В зависимости от их конфиденциальности резервное копирование данных будет выполняться разными способами и разными способами. в среднем.

Публичные данные

Данные, содержащиеся в этой категории, не имеют существенно большего объема и не меняются так часто, как другие данные. На мой взгляд, для большей части этих данных можно создать резервную копию с

помощью службы Dropbox, потому что дело только в том, чтобы не потерять их. Так что не имеет значения, если сотрудники будут иметь к ним доступ из любого места. Для этих данных я бы рекомендовал сделать полную резервную копию только в случае каких-либо изменений.

Внутренние данные

Внутренние данные представляют собой большую часть информационных активов компании. Для этих данных я бы чтобы сократить время, необходимое для создания резервной копии, он рекомендовал выбрать дифференциальную резервную копию. При резервном копировании будет передано значительно меньше данных, чем, например, в случае полного резервного копирования. В идеале самая старая версия резервной копии будет использоваться в качестве снимка, к которому они будут постепенно добавляться. Я рекомендую делать резервную копию этих данных каждый день в полночь. Полное резервное копирование также будет выполняться раз в неделю, и последние 5 резервных копий будут сохранены. Для резервного копирования внутренних данных компании я бы выбрал хранилище данных с сетевым подключением. Хранилище (NAS). В настоящее время ящики NAS можно приобрести по относительно разумной цене (в сегодняшних время дешевле, чем классический стоечный сервер), и в них можно использовать HDD диски с сервера, которые в настоящее время содержат архивную резервную копию, но какая компания в планах выключить (это два диска 2TB 3.5 "SATA II 7200rpm). Эти диски затем будут возможность зеркалирования (RAID 1) для повышения надежности резервного копирования. Большим преимуществом также является подключение этого хранилища данных в локальную сеть (LAN), что способствует очень хорошей доступности сохраненных данных. Система NAS будет накапливать данные работников за день и в полночь будет

синхронизироваться с облачной копией хранящейся на облачном FTP https://lancloud.ru.

Кроме того, все данные будут зашифрованы перед выполнением резервного копирования, что достигается так же с помощью сервиса https://lancloud.ru. Всегда будут храниться 3 последних версии этой резервной копии. Исходные коды системы будут храниться в системе управления версиями SVN, чьё Резервное копирование описано в следующем подразделе.

3.3 Резервное копирование SVN

Данные из SVN будет скопировано на FTP-сервер. Поэтому необходимо выбрать программное обеспечение или утилиту, которая может работать в системах, использующих ядро Linux. В настоящее время используется утилита RDIFF_backup, которая использует протокол SSH для передачи данных. Лучшим вариантом здесь,по моему мнение, будет утилита Duplicity, которая использует алгоритм rsync, который полезен для синхронизации с FTP-сервером, чтобы в результате были только новые, или измененные файлы. Двойственность может:

– упаковать файлы в архив (.tar),

– обезопасить этот архив (шифрование и подпись с помощью GPG),

– сделать дифференциальную резервную копию на FTP,

– что в точности соответствует потребностям компании в создании этой резервной копии.

3.4 Выбор технологий

В этом подразделе я сосредоточусь на выборе конкретных технологий, которые потребуются. для выполнения резервного копирования с помощью системы, которую я разработал. Для наглядности

представляю здесь список необходимых технологий: Устройства NAS В качестве устройства NAS я бы выбрал для компании: Сетевое хранилище QNAP D2.

Код: 470545; отсеков для дисков: 2; интерфейс: SATA III; форм-фактор: 2.5"/3.5"; LAN: 2 x 10/100/1000 Мбит/с; портов USB3.0: 3; RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, горячая замена дисков; совместимо с IP-камерами

Это внешний бокс для 2 жестких дисков 3,5 дюйма SATA II/III, поддерживающих RAID 0 и RAID 1. Коробка поставляется без установленный жесткий диск и в настоящее время доступен через интернет-магазин https://www.citilink.ru/ по цене 17690 руб.

Рисунок 8 – Сетевое хранилище QNAP D2

Преимущество Накопителя NAS заключается в том, что можно будет использовать диски с сервера, который компания планирует отключать после развертывание архивной копии через FTP.

FTP сервер

FTP-сервер с емкостью будет предоставлен https://lancloud.ru, поэтому покупать не нужно. в этом случае нет оборудования.Компаниябудет платить только ежемесячную плату за Работу FTP-сервера.Эти ежемесячные платежи должны составлять около 1000 рублей в месяц. в зависимости объёма резервных копий.

Программа для выполнения дифференциального резервного копирования по FTP

Я выбрал утилиту Duplicity для выполнения резервного копирования по FTP.Эта утилита находится в свободном доступе для скачать на домашней странице проекта Duplicity. В результате вам нужно будет только приобрести NAS-бокс и заплатить ежемесячная плата за работу FTP-сервера.На мой взгляд, этот вариант внесет значительный вклад компания, чтобы сэкономить деньги. В следующей таблице указана общая сумма необходимых средств. потратить на покупку необходимых технологий (но не включает ежемесячную плату за Работа FTP-сервера)

3.5 Принципы информационной безопасности и их организационная интеграция

Рекомендую компании потребовать от всех сотрудников в интересах информационной безопасности строгое соблюдение следующих принципов. Будет определено, кто именно отвечает за соблюдение принципов контроля за их соблюдением и возможные санкции. На основании требования к безопасности информации, указанные в стандарте CSN ISO / IEC 27001

Эта Директива будет содержать следующие принципы:

1. Сотрудник входит во внутреннюю сеть компании, используя имя пользователя а пароли, которые знает только он, и категорически запрещено передавать эту информацию другому лицу, или каким-либо образом предоставить другому лицу доступ к информации через его учетную запись.

2. Сотрудник обязан использовать безопасное соединение при доступе к информации.

3. Сотрудник не может использовать чужую учетную запись пользователя для доступа к информации.

4. Весь доступ к данным регистрируется и отслеживается сотрудником. несет ответственность за всю работу с данными, выполняемую через него учетная запись пользователя.

5. Пароли пользователей генерируются компьютером автоматически и состоят из больших и строчных букв и цифр. После первого входа в систему у сотрудника обязательство сменить пароль, при этом новый пароль также должен состоять из больших и строчных букв и цифр. Минимальная длина пароля - 9 символов.

6. Сотрудник не должен хранить пароль в приложениях (например, в веб-браузере) для следующего использования. Ответственное лицо: сотрудник Контроль осуществляет: менеджер по информационной безопасности. Штрафы: неоднократные или особо серьезные нарушения любой из этих директив влекут письменное наказание. выговор работнику в случае повторного выговора в течение 6 месяцев, с ним это возможно в соответствии с Законом № 262/2006. прекратить трудовые отношения Директива: Директива по информационной безопасности - контроль доступа к данным

3.6 Использование аппаратного и программного обеспечения

Эта Директива будет содержать следующие принципы:

1. Если не указано иное, сотрудник не без предварительного согласия Superior может каким-либо образом изменять конфигурацию программного обеспечения, используемого на работе.

2. В случае подозрения или обнаружения дефекта оборудования или программного обеспечения работник обязан немедленно сообщить об этом уполномоченному лицу.

3. При работе с данными сотрудник может использовать только то оборудование и программное обеспечение, которое ему доступно. предоставлены компанией для выполнения работ. Использование любого другого программного обеспечения должно заранее согласовываться с сотрудниками.

4. На компьютере каждого сотрудника должна быть установлена антивирусная программа, предоставляется компанией и регулярно обновлять эту программу.

Ответственное лицо: сотрудник

Осмотр осуществляет: непосредственный руководитель Санкции: при обнаружении первого нарушения на компьютер сотрудника будет установлено программное обеспечение. следить за его активностью, которая будет активна на протяжении всей его работы; несколько раз или особенно серьезное нарушение повлечет за собой письменное предупреждение сотруднику; если это в течение 6 месяцев работнику неоднократно оговариваются выговоры, с ним это возможно в соответствии с Законом No. 262/2006 Сб прекратить трудовые отношения

Директива: Директива по информационной безопасности - использование оборудования и программного обеспечения

3.7 Процесс резервного копирования

Эта Директива будет содержать следующие принципы:

1. Сотрудник обязан поддерживать свою переписку по электронной почте как с клиентами, так и с с другими сотрудниками компании.

2. Резервное копирование SVN необходимо производить ежедневно на FTP-сервер в 3 часа ночи.

3. Провайдер FTP-сервера не имеет права каким-либо образом манипулировать данными компании. хранятся на этом сервере, если это прямо не разрешено компанией. Также отвечает за безопасность хранимых данных и надежность резервного копирования.

4. Контракты с клиентами и счета-фактуры должны храниться как в бумажной, так и в электронной форме. форма. Эти документы отправляются на центральную почту для управления счетами в формате pdf.

5. Резервные копии внутренних и общедоступных данных на устройстве NAS создаются ежедневно в полночь.

6. Сотрудникам разрешается хранить данные только в той службе Dropbox, которая классифицируется как общедоступный.

7. Секретные данные, для которых выполняется электронное резервное копирование, копируются отдельно от другие данные (на магнитных лентах) и шифруются перед выполнением резервного копирования.

Ответственное лицо: сотрудник, руководитель проекта соответствующего отдела, руководитель информационная безопасность, провайдер FTP-сервера Контроль осуществляют: менеджер по информационной безопасности, руководитель. Санкции: неоднократные или грубые нарушения приводят к письменному предупреждению сотрудника; если сотруднику неоднократно делали выговор в течение 6 месяцев, с ним можно по Закон № 262/2006 Coll.прекратить трудовые

отношения;в случае нарушения принципа № 3 Поставщик FTP-сервера, компания может отказаться от договора Директива: Директива по информационной безопасности - процесс резервного копирования

3.8 Физическая и экологическая безопасность

Эта Директива будет содержать следующие принципы:

1. Для доступа в офисы компании сотрудник использует чип-карту, без которой невозможно добраться из офисов. Эта карта не может быть предоставлена сотрудником третьим лицам.

2. Сотрудник не может использовать смарт-карту другого человека для доступа в офис.

3. Если сотрудник покидает офис последним, он обязан включить сигнализацию. используя код. У каждого сотрудника свой код.

4. В случае утери или кражи чип-карты работник обязан немедленно уведомить менеджера по информационной безопасности.

5. Сотрудник всегда обязан правильно выйти из всех систем и приложений в конце его рабочего времени.

6. Устройство NAS находится в запертой комнате, доступ к которой имеет только агент, компания и менеджер по информационной безопасности.

Ответственное лицо: сотрудник, руководитель проекта соответствующего отдела, руководитель информационной безопасности Контроль осуществляют: менеджер по информационной безопасности, руководитель.

Санкции: если в результате нарушения данных принципов необходимо потратить средства на возобновление охранных помещений компании, виновник оплачивает их из своей заработной платы;Любые нарушение приводят к письменному предупреждению сотрудника;если

сотруднику объявили выговор повторно в течение 6 месяцев, с ним возможно расторжение трудового договора.

3.9 Безопасность человеческих ресурсов

Эта Директива будет содержать следующие принципы:

1. Каждый сотрудник должен пройти инструктаж по технике безопасности во время его прикомандирования. информация и способы обработки каждой категории информации. Он также узнает о соблюдении физической безопасности, правилах использования. оборудование и программное обеспечение и как работать с учетными записями пользователей и паролями.

2. После прохождения обучения сотрудник обязан подписать письменное заявление о том, что прошел обучение и согласен придерживаться принципов безопасной работы с информацией.

3. Работник обязан во время трудовых отношений всегда и без исключения соблюдать руководящие принципы и стандартные процедуры, установленные компанией.

4. После увольнения работник обязан подать аванс. электронная переписка с менеджером по информационной безопасности. Он также должен представить все документы он использовал на работе.

5. В случае увольнения менеджер по информационной безопасности заблокирует все права доступа, которые имел сотрудник в компании. Ответственное лицо: сотрудник, менеджер по информационной безопасности Контроль осуществляют: менеджер по информационной безопасности, непосредственный руководитель сотрудника. Санкции: в случае нарушения любого из этих принципов сотрудник должен пройти переподготовку. по теме информационной безопасности за свой счет Директива: Директива по информационной безопасности - безопасность человеческих ресурсов.

ЗАКЛЮЧЕНИЕ

Целью данной работы было создание подходящей стратегии резервного копирования и безопасности данных для образовательной организации. При разработке данной стратегии необходимо было учесть изменения, внесенные компанией. Планируется внедрить, особенно желание компании использовать возможность аренды FTP при резервном копировании данных сервер от https://lancloud.ru. Выбранные методы резервного копирования данных различаются в зависимости от конфиденциальности этих данных. Для резервного копирования Для общих внутренних данных я выбрал сетевое устройство хранения данных, в основном из-за его простоты и доступности. Данные, хранящиеся на этом устройстве, доступны по локальной сети, что, несомненно, желательно в случае постоянно обрабатываемых данных.

Секретные данные, потеря или разглашение которых может иметь серьезные или фатальные последствия для компании, рекомендуется выполнять резервное копирование отдельно от других данных и даже не резервировать некоторые в электронном виде вообще.

Чтобы процесс резервного копирования и связанная с ним общая информационная безопасность были эффективными, необходимо установить определенные принципы, которым должны следовать все сотрудники в интересах безопасности информации Поэтому я попытался предложить руководящие принципы, определяющие эти принципы и они также определяют, кто несет ответственность за их соблюдение и что угрожает в случае несоблюдения санкции. В заключительной части предложения я коснулся плана выхода из кризиса. Пусть компания однако сильные политики информационной безопасности, сбои и различные сбои вероятно, время от времени не ускользнет, поэтому важно иметь предварительный план чтобы справиться с этими ситуациями. Разработка

такого плана в целом настолько сложна, что Можно обойтись в рамках этой работы. Поэтому я попытался предложить хотя бы упрощенная версия этого плана, в случае аварии с первичными данными

СЛОВАРЬ ТЕРМИНОВ

Авария – неумышленное происшествие с деструктивным воздействием на объект.

Авторизация – формирование профиля прав для конкретного участника информационной верификации.

Атака – попытка практической реализации угрозы (успешная или нет).

Аудит – это анализ накопленной информации, проводимый в реальном времени или периодически.

Аутентификация – обеспечение уверенности в том, что участник информационной верификации идентифицирован верно.

Аутсорсинг – Выполнение отдельных задач проекта компании сторонними организациями, специализирующимися в этой области.

Базы данных – организованная структура, предназначенная для хранения, изменения и обработки взаимосвязанной информации, преимущественно больших объемов.

Безопасность информации – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

Безопасность информационной технологии – защищенность технологического процесса переработки информации.

Биометрическая аутентификация – Аутентификация, опирающаяся на уникальные биологические показатели человека. К основным биометрическим идентификаторам относятся отпечатки

пальцев, рукописные подписи, образцы голоса, результаты сканирования сетчатки и радужной оболочки глаза, формы ладони или черт лица.

Браузер – Программа, обеспечивающая доступ к текстовым и графическим страницам World Wide Web.

Верификация (проверка) цифровой подписи документа – Проверка соотношения, связывающего хэш-функцию документа, подпись под этим документом и открытый ключ подписавшего пользователя. Если рассматриваемое соотношение оказывается выполненным, то подпись признается действительной, а сам документ — подлинным, в противном случае документ считается измененным, а подпись под ним — недействительной.

Взаимная (перекрестная) сертификация – двусторонний процесс сертификации двух доверенных удостоверяющих центров.

Вирус – вредоносная программа, которая кроме выполнения деструктивных действий может автоматически размножаться (возможно, с самомодификацией) и распространяться на новые информационные системы.

Владелец информации – Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.

Владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Вредоносная программа – некоторый программный код (модуль, скрипт, макрос), созданный с целью нарушения информационной безопасности.

Дешифрование – восстановление с помощью ключа исходной информации.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях. К ВТСС относятся: телефонные средства и системы; средства и системы передачи данных, системы радиосвязи; средства и системы охранной и пожарной сигнализации; средства и системы оповещения и сигнализации; контрольно-измерительная аппаратура; средства и системы кондиционирования; средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания, телевизоры и радиоприемники и т.п.); средства электронной оргтехники; иные технические средства и системы.

Выпуск сертификата – Генерация сертификата и уведомление владельца, зафиксированного в нем, о подробном содержании этого сертификата.

Депонирование ключей – Предоставление копий секретных ключей третьей стороне и разрешение пользоваться ими при определенных обстоятельствах, в качестве третьей стороны чаще всего выступают правительственные учреждения и правоохранительные органы. Депонирование ключей может быть возложено на независимое подразделение внутри организации, развертывающей PKI, или на внешнее агентство.

Доверяющая сторона – Лицо, которое получает сертификат и полагается на него при совершении сделок или обмене сообщениями.

Доказательство доставки данных – Атрибут сервиса неотказуемости. Гарантирует, что сторона, принимающая информацию, не сможет отрицать того, что получила сообщение.

Доказательство происхождения данных – Атрибут сервиса неотказуемости. Гарантирует, что сторона, отправляющая информацию, не сможет отрицать того, что сообщение отправлено ей.

Документ – Документированная информация, снабженная определенными реквизитами.

Документированная информация – Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Домен безопасности – Группа (компания, рабочая группа или коллектив), сертификаты которой выпущены одним и тем же удостоверяющим центром.

Домен доверия –Множество субъектов, сертификаты которых выпущены одним и тем же удостоверяющим центром. Пользователи, чьи сертификаты подписаны данным удостоверяющим центром, могут полагаться на идентичность (действительность, подлинность) другого пользователя, который владеет сер¬тификатом, выпущенным тем же удостоверяющим центром.

Дополнения сертификата – Необязательные атрибуты сертификата, позволяющие включать в сертификат информацию, которая отсутствует в основном содержании сертификата.

Доступ к информации (доступ) – ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации.

Доступ к ресурсу – получение субъектом доступа возможности манипулировать (использовать, управлять, изменять характеристики и т.п.) данным ресурсом.

Доступность – возможность получения авторизованного доступа к информации со стороны уполномоченных лиц.

Заверение (нотаризация) – Регистрация данных у доверенного третьего лица для повышения уверенности в правильности таких характеристик, как содержание, источник данных, время доставки.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Закрытая система PKI – Характеризуется наличием договоров, определяющих права и обязанности всех участников системы в отношении аутентификации сообщений или транзакций.

Закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

Защита информации от несанкционированного доступа (защита от НСД) или воздействия – деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию).

Защищаемые помещения (ЗП) – помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

Злоумышленник – субъект, преследующий корыстные или деструктивные цели, противоречащие целям системы.

Иерархия доверия – Система проверки цифровых сертификатов. Каждый сертификат связан с сертификатом ключа подписи того субъекта, который снабдил его цифровой подписью. Так, сертификат абонента связан с сертификатом УЦ низшего уровня, который, в свою очередь, связан с сер¬тификатом УЦ более высокого уровня и так далее до УЦ высшего уровня. Следуя по цепочке доверия до известной доверенной сторо¬ны, можно убедиться в действительности сертификата.

Идентификатор – уникальный набор символов, однозначно соответствующий объекту или субъекту в данной системе .

Идентификация – распознавание участника процесса информационного взаимодействия перед тем, как к нему будут применены какие-либо аспекты информационной бзопасности.

Информация – данные, представленные в виде, пригодном для хранения, обработки и передачи, и представляющие определенную ценность.

Информационная безопасность – комплекс мероприятий по защите информации и обеспечению безопасного функционирования информационной системы.

Информационное пространство – совокупность информационных систем, взаимодействующих между собой, причем одна часть этих систем может иметь интересы, прямо противоположные интересам другой.

Информационная система – совокупность объектов и субъектов информационного взаимодействия.

Информативный сигнал – Электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация, передаваемая, хранимая или обрабатываемая в основных технических средствах и системах или обсуждаемая в ЗП.

Информационная система общего пользования – информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Информационные сети общего пользования (Сети) – вычислительные (информационно-телекоммуникационные) сети открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано.

Инфраструктура открытых ключей (ИОК) – Технологическая инфраструктура и сервисы, гарантирующие безопасность информационных и коммуникационных систем, использующих алгоритм с открытыми ключами.

Клиентская часть – запускается на машине злоумышленника, который, связавшись с серверной частью, может выполнять различные действия: изменение файлов, чтение информации с монитора, контроль вводимых и выводимых данных.

Компрометация ключей – Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

Контролируемая зона (КЗ) – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств. Границей КЗ могут являться: периметр охраняемой территории организации; ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории. В отдельных случаях, на период обработки техническими средствами конфиденциальной информации, границы КЗ временно могут расширяться. При этом должны приниматься организационные и технические меры, исключающие или существенно затрудняющие возможность ведения перехвата информации в этой зоне.

Контроль доступа (управление доступом) – Процесс ограничения доступа к ресурсам системы только разрешенным субъектам или объектам.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

Корневой удостоверяющий центр – Удостоверяющий центр, находящийся на вершине иерархии в инфраструктуре открытых ключей, выпускает самоподписанный сертификат и сертификаты для подчиненных удостоверяющих центров.

Корпоративная информационная система – информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Криптографическая защита – Защита данных при помощи криптографического преобразования данных.

Криптографические операции – безопасное хеширование; выработка и верификация контрольных сумм (имитовставки); зашифрование и (или) расшифрование данных; зашифрование и (или) расшифрование криптографических ключей, выработка и верификация электронной цифровой подписи.

Криптографический ключ – Последовательность символов, которая контролирует криптографические операции (зашифрование, расшифрование, вычисление хэш-функции, вычисление или проверку цифровой подписи).

Криптографический модуль – Комплекс программных, программно-аппаратных и аппаратных средств, используемый с целью гарантирования безопасности при генерации, хранении и применении криптографического ключа.

Криптографическое преобразование – Преобразование данных при помощи шифрования и (или) выработки имитовставки.

Криптосистема с открытыми ключами – Система построенная на основе асимметричного криптографического алгоритма, использующего два ключа (открытый ключ и секретный ключ), соответствующих друг другу. Если информация зашифровывается одним ключом (открытым), система может расшифровать ее при помощи другого ключа (секретного). Аналогично, если информация подписывается одним ключом (секретным), абонент может использовать другой ключ (открытый) для аутентификации лица, поставившего подпись. Атрибуты этих двух ключей не позволяют вычислить секретный ключ, даже если известен открытый ключ.

Локальная вычислительная сеть (ЛВС) – совокупность основных технических средств и систем, осуществляющих обмен информацией между собой и с другими информационными системами, в том числе с ЛВС, через определенные точки входа/выхода информации, которые являются границей ЛВС.

Маскировка – методы криптографической и стеганографической защиты.

Межсетевой экран (МЭ) – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и (или) выходящей из АС. МЭ обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе

заданных правил, проводя, таким образом, разграничение доступа субъектов из одной АС к объектам другой АС.

Модель доверия – Модель, задающая порядок сертификации одних удостоверяющих центров другими.

Мостовой удостоверяющий центр – Удостоверяющий центр, предназначенный для установления связей между разнородными инфраструктурами открытых ключей.

Набор положений PKI – Совокупность положений практики и/или политики PKI, охватывающих круг стандартных тем для формулирования политики применения сертификатов или регламента.

Нарушитель – это лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Некорректный электронный документ – Электронный документ, не прошедший процедуры расшифрования данных, проверки электронной цифровой подписи информации, контроля формата документов, а также документ, имеющий искажения в тексте сообщения (наличие символов, букв или цифр в расшифрованном (открытом) тексте документа, не позволяющих понять его смысл).

Неотрекаемость – предполагает, что отправитель информации не может отречься от факта отправления, а получатель – от факта получения.

Неотказуемость получения – Невозможность для получателя отрицать прием информации, поскольку свидетельство получения (например, цифровая подпись) доказывает связь между атрибутами получателя и информацией.

Несанкционированное действие – действие субъекта в нарушение установленных в системе правил обработки информации.

Несанкционированный доступ – это преднамеренное овладение конфиденциальной информацией неуполномоченным лицом.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации. В контексте настоящего документа к ним относятся АС различного уровня и назначения на базе СВТ, средства и системы связи и передачи данных, включая коммуникационное оборудование, используемые для обработки и передачи конфиденциальной информации.

Открытая система PKI – Характеризуется отсутствием формальных договоров, регулирующих отношения субъектов системы.

Открытый ключ – Криптографический ключ, который связан с секретным с помощью особого математического соотношения. Открытый ключ известен всем другим пользователям системы и предназначен для про¬верки электронной цифровой подписи и расшифрования, позволяет определить автора подписи и достоверность электронного документа, но не позволяет вычислить секретный ключ.

Открытый ключ электронной цифровой подписи — уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Ошибка – непреднамеренное незапланированное действие, совершаемое субъектом, которое представляет или может представлять угрозу информационной безопасности.

Пароль – секретный набор символов, позволяющий подтвердить соответствие субъекта предъявленному им идентификатору.

Пара ключей (ключевая пара) – Открытый ключ, используемый в криптосистеме с открытыми ключами, и соответствующий ему секретный (закрытый) ключ.

Побуждение – такой метод защиты, который побуждает пользователей и персонал системы не нарушать сложившиеся моральные нормы.

Подписчик (владелец) сертификата – Лицо, которое заключает с удостоверяющим центром договор об обслуживании и становится владельцем сертификатов, выпущенных УЦ.

Подтверждение подлинности электронной цифровой подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Политика (Правила) применения сертификатов – Установленный набор правил, характеризующих возможность применения сертификата определенным сообществом и/или для класса приложений с определенными требованиями безопасности. Политика применения сертификатов позволяет доверяющей стороне оценить надежность использования сертификата для определенного приложения.

Пользователь сертификата ключа подписи – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе.

Препятствие – метод физического преграждения пути злоумышленнику к ресурсам информационной системы.

Принуждение – метод защиты, при использовании которого пользователи и персонал информационной системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Приостановление сертификата – Временное аннулирование сертификата в период его действия с последующим его возобновлением или отзывом.

Провайдер Сети – уполномоченная организация, выполняющая функции поставщика услуг Сети для абонентов Сети.

Программная закладка – вредоносная программа, реализованная как одна из скрытых функций системы.

Профиль – набор установок и конфигураций для данного субъекта или объекта и определяющий его работу в информационной системе.

Профиль сертификата – Набор характеристик, которые задают тип данного сертификата.

Путь доверия – Связывает доверяющую сторону с одной или многими третьими доверенными сторонами и позволяет конфиденциально проверять законность используемого доверяющей стороной сертификата.

Разглашение – это умышленные или неосторожные действия с конфиденциальной информацией, приведшие к ознакомлению с ней неуполномоченных лиц. Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена информацией.

Разграничение доступа к ресурсам АС – это такой порядок использования ресурсов системы, при котором субъекты получают доступ к объектам в строгом соответствии с установленными правилами.

Разностный список аннулированных сертификатов – Список, фиксирующий изменения списка аннулированных сертификатов, произошедшие с момента выпуска последнего.

Расшифрование данных – Процесс преобразования зашифрованных данных в открытые при помощи шифра.

Регистрационный центр (РЦ) – Лицо (физическое или юридическое), которое с санкции удостоверяющего центра выполняет функции аутентификации в процессе выпуска или аннулирования сертификата. Регистрационный центр не выпускает сертификаты и не ведет списки аннулированных сертификатов.

Регламент УЦ – Документ, который устанавливает и детализирует процедуры сертификации и управления ключами в соответствии с политикой удостоверяющего центра.

Риск – фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери — прямые или косвенные).

Секретный (закрытый) ключ – Ключ асимметричной ключевой пары, который доступен только одному пользователю системы и хранится им в тайне. В системе цифровой подписи определяет криптопреобразование подписи, в асимметричной системе шифрования определяет криптопреобразование расшифрования.

Сервер восстановления ключей – Сервер инфраструктуры открытых ключей, который поддерживает создание резервных копий и восстановление ключей шифрования конечных субъектов.

Сервер каталогов – Сервер инфраструктуры открытых ключей, который хранит информацию о сертификатах и атрибутах субъектов сертификатов открытых ключей.

Сервер сертификатов (центр сертификации) – Сервер инфраструктуры открытых ключей, на который возлагаются функции выпуска и управления сертификатами, защищенного хранения секретного ключа удостоверяющего центра, поддержки жизненного цикла сертификатов и ключей, восстановления данных, ведения контрольного журнала и регистрации всех операций удостоверяющего центра.

Сервисы безопасности – Совокупность механизмов, процедур и других средств управления для снижения рисков, связанных с угрозой утраты или раскрытия данных.

Сервис неотказуемости – Сервис предотвращения отказа от участия в обмене информацией, гарантирующего, что стороны, отправляющие и принимающие электронные сообщения или докумен¬ты, не смогут отрицать свое участие в информационном обмене в целом или на отдельных его этапах.

Сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи. Содержит информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, о выпустившем удостоверяющем центре и т.д.

Сертификат сервера – Цифровой сертификат, выпущенный удостоверяющим центром для web-сервера. Предназначен для аутентификации web-сервера при выполнении транзакций, основанных на протоколах TLS/SSL.

Сертификат средств электронной цифровой подписи – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

Сертификация (открытых ключей) – Процесс выпуска сертификатов и их последующего обслуживания для физических и юридических лиц, оборудования и т.д.

Система асимметричного шифрования – Система, основанная на асимметричных методах, когда преобразование с открытым ключом используется для шифрования, а соответствующее преобразование с закрытым ключом — для расшифрования.

Система защиты АС (информации) – совокупность (комплекс) специальных мер правового (законодательного) и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения безопасности АС (циркулирующей в АС информации).

Служебная информация СЗИ НСД – информационная база АС, необходимая для функционирования СЗИ НСД (уровень полномочий эксплуатационного персонала АС, матрица доступа, ключи, пароли и т.д.).

Согласование ключа – Процесс установления общего ключа для взаимодействия между пользователями, при котором ни один из пользователей не может предопределять значение этого ключа.

Специальный защитный знак (СЗЗ) – сертифицированное и зарегистрированное в установленном порядке изделие, предназначенное для контроля несанкционированного доступа к объектам защиты, определяя подлинность и целостность СЗЗ, путем сравнения самого знака или композиции «СЗЗ — подложка» по критериям соответствия

характерным признакам визуальными, инструментальными и другими методами.

Список аннулированных (отозванных) сертификатов (CAC/COC) – Список недействительных сертификатов, генерируется удостоверяющим центром.

Средства электронной цифровой подписи – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций — создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Техническая защита конфиденциальной информации (ТЗКИ) – защита информации некриптографическими методами, направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и от специальных воздействий на информацию в целях ее уничтожения, искажения или блокирования.

Технический канал утечки информации – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Токен – Устройство хранения криптографических ключей, аппаратный ключ.

Транспортировка ключа – Защищенный процесс передачи ключа от одного пользователя к другому.

Троянская программа – вредоносная программа, выполняющая несанкционированные и недокументированные действия.

Угроза – возможность реализации несанкционированных действий в отношении информационной системы.

Удостоверяющий центр (УЦ) – Доверенное лицо (физическое или юридическое), которое выпускает, публикует, аннулирует сертификаты, приостанавливает их действие.

Управление доступом – метод защиты информации регулированием использования всех ресурсов информационной системы.

Управление ключами – Создание (генерация) ключей, их хранение, распространение, удаление (уничтожение), учет и применение в соответствии с политикой безопасности.

Услуги Сети – комплекс функциональных возможностей, предоставляемых абонентам сети с помощью прикладных протоколов (протоколы электронной почты, FTP — File Transfer Protocol — прием/передача файлов, HTTP — Hyper Text Transfer Protocol — доступ к Web-серверам, IRC — Internet Relay Chat -диалог в реальном времени, Telnet терминальный доступ в сети, WAIS — Wide Area Information Servers — система хранения и поиска документов в сети и т.д.).

Утечка – это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена по техническим каналам.

Учёт – фиксация и анализ всех действий уполномоченных лиц, выполняемых ими в рамках, контролируемых системой информационной безопасности.

Уязвимость информации – подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности, или неправомерному ее тиражированию.

Хеш-код (дайджест) – Строка битов фиксированной длины, полученная из строки битов произвольной длины при помощи математической операции над данными, является выходом хэш-функции.

Хэш-функция – это труднообратимое преобразование данных, реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хэш-функции.

Целостность – состояние информации, при котором изменять её могут только уполномоченные лица.

Цифровая подпись (ЭЦП) – Результат криптографического преобразования, при котором дайджест (хеш-код) подписываемого сообщения шифруется секретным (закрытым) ключом. Цифровая подпись может быть проверена путем сопоставления значения, расшифрованного при помощи открытого ключа, и дайджеста (хеш-кода) исходного сообщения. Цифровая подпись может быть выработана только лицом, имеющим секретный ключ — результат ее использования в электронном документообороте аналогичен собственноручной подписи на бумажном документе.

Шифровальный ключ (симметричный) – Параметр, используемый в симметричном криптографическом алгоритме, позволяющий отправителю и получателю использовать один и тот же криптографический ключ для зашифрования и расшифрования данных.

Шифрование – преобразование информации в форму, при которой невозможно или существенно затруднено извлечение из неё осмысленных данных без ключа.

Шифротекст – Зашифрованная информация.

Экран – это средство разграничения доступа клиентов из одного множества информационных систем к серверам из другого множества посредством контроля информационные потоков между двумя

множествами систем Контроль потоков состоит в их фильтрации и выполнении некоторых преобразований.

Электронная цифровая подпись (ЭЦП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронный документ – Задокументированная совокупность данных, представленных в электронно-цифровой форме и зафиксированных на материальном носителе с реквизитами, позволяющими идентифицировать эту информацию и авторов документа. Идентификация электронного документа обеспечивается средствами защиты на основе алгоритмов шифрования, электронной цифровой подписи и защиты от несанкционированного доступа.

СПИСОК ЛИТЕРАТУРЫ

1. Пусто, А.Г. Быстрый старт TCP / IP: Основы интернет-протокола. – 2-е изд. – Сан-Франциско: Sybex Inc., 2002. – 320 с.

2. Доседел, Т. Компьютерная безопасность и защита данных. – 1-е изд. – Брно: Компьютер Press, 2004. – 190 с.

3. Гилфиллан, И. Мы думаем в MySQL 4 : Библиотека программиста. – 1-е издание. – Прага: Града, 2003. – 750 с.

4. Грегори, П.Х. Планирование аварийного восстановления информационных технологий для чайников. – Хобокен, Нью-Джерси: Уайли, 2008. – 360 с.

5. Хикс, М. Cisco: Оптимизация приложений. – Прага: Града, 2008. – 336 с.

6. Hontañón, R. J. Linux: практическая безопасность. – 1-е изд. – Прага: Града, 2003. – 438 с.

7. Кастнер, А. Резервное копирование и архивирование. – Прага: ГКомп, 1997.

8. Krčmá, P. Linux: построить компьютерную сеть. – 1-е изд. – Прага: Града, 2008. – 182 с.

9. Mlýnek, J. Безопасность деловой информации. – Брно: Компьютерная пресса, 2007.

10. Пециновский, Ю. Архивирование и сжатие данных. – Прага: Герд, 2003.

11. Родричова, Д., Сташа, П. Информационная безопасность как условие процветание компании. – 1-е издание. – Прага: Града, 2002.

12. Wallace, M., Webber L. Руководство по аварийному восстановлению: пошаговый план обеспечить непрерывность бизнеса и защитить жизненно важные операции, объекты и активы. – 2-е изд. – Нью Йорк: Американская ассоциация менеджмента, 2011. – 440 с.

13. Войтов, Н.М. Администрирование Red Hat Enterprise Linux : Учебное пособие / Н.М. Войтов. – ДМК Пресс, 2011.

14. Гультяев, А.К. Восстановление данных / А.К. Гультяев. – СПб.: Питер, 2005.

15. Казаков, В.Г. Разработка программной файлово-ориентированной системы резервного копирования данных / В.Г. Казаков, С.А. Федосин // Технологии Microsoft в теории и практике программирования : материалы конф. / под ред. проф. Р. Г. Стронгина. – Н. Новгород : Изд-во Нижегор. гос. ун-та, 2007. – С. 108-110.

16. Кенин, А.М. Самоучитель системного администратора /А.М. Кенин. – СПб.: БХВ-Петербург, 2012.

17. Куртис Престон, В. Резервное копирование и восстановление Unix, O'Reilly&Associates / В. Куртис Престон.

18. Макарова, Н.В. Информатика 9 / Н.В. Макарова. – СПб: Питер, 2007.

19. Мюллер, С. «Модернизация и ремонт ПК» / С. Мюллер. – «Вильямс», 2007.

20. Мюллер, С. «Модернизация и ремонт ПК» / С. Мюллер. – 17 изд. – «Вильямс», 2007.

21. Руководство по системному администрированию Red Hat Enterprise Linux. – Издательство Red Hat, 2005.

22. Симонович, С., Евсеев, Г. Эффективная работа: познай свой компьютер / С. Симонович, Г. Евсеев. – СПб.: Питер, 2005.

23. Хорев, П. Программно – аппаратная защита информации : Учебное пособие / П. Хорев. – «Форум», 2009.

24. Хорев, П. Программно-аппаратная защита информации : учебное пособие. – «Форум», 2009.

25. Чекмарев, А.Н., Вишнякова, Д.Б. Восстановление системы. Процедуры резервного копирования и восстановления // Microsoft

Windows 2000: Server и Professional. Русские версии / А.Н. Чекмарев, Д.Б. Вишнякова. – Глава 8. – Санкт-Петербург, 2000.

26. Шаньгин, В. «Защита компьютерной информации. Эффективные методы и средства» / В. Шаньгин. – «ДМК Пресс», 2010.

27. Шаньгин, В. Защита компьютерной информации. Эффективные методы и средства / В. Шаньгин. – «ДМК Пресс», 2010.

28. Шапиро, Д, Бойс, Д. Архивация и восстановление данных // Windows 2000 Server. Библия пользователя. Windows 2000 Server. Bible. – Глава 17. – Москва: Компьютерное издательство «Диалектика», Торговый дом «Вильямс», 2001.

Стандарты

29. Информационные технологии. – Методы безопасности: Системы управления информационной безопасностью. – Требования.

Электронные ресурсы

30. Небольшой обзор носителей резервных копий [Электронный ресурс]. Режим доступа: http://www.ictsecurity.cz/09/09/2-zalohovani/maly-prehled-zalohovacichmedii.html

31. Определение и ротация авансов [Электронный ресурс]. Режим доступа: http://www.storage.cz/index.php?option=com_content&task=view&id =47&Itemid=41

32. Резервное копирование и синхронизация данных между компьютерами [Электронный ресурс]. Режим доступа: http://www.root.cz/clanky/dropbox-zaloha-a-synchronizace-datmezi-pocitaci/ (Дата обращения: 13.05.2020)

33. Сравнение контроля версий ПО [Электронный ресурс]. Режим доступа: http://www.timedoctor.com/biz3.0/gitmecurial-and-cvs-comparison-of-svn-software (Дата обращения: 01.02.2021)

34. Техническая документация с официальных источников (сайт разработчиков GFI backup) [Электронный ресурс]. Режим доступа: www.gfi.ru

35. Техническая документация с официальных источников (сайт разработчиков Paragon Drive backup Workstation) [Электронный ресурс]. Режим доступа: www.paragon.ru

36. Техническая документация с официальных источников (сайт разработчиков продуктов Acronis) [Электронный ресурс]. Режим доступа: www.acronis.ru

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. «Резервное копирование данных в локальной вычислительной сети в современных условиях»

Королева Яна Васильевна, Шалаев Александр Дмитриевич.

Научный руководитель: *к.п.н., Зайцев Владимир Сергеевич*

В сборнике XI Международной научно-практической конференции «Наука и инновации в XXI веке: актуальные вопросы, открытия и достижения». – Пенза, 2018. – Ч. 1. – С. 103.

2. «Информационная безопасность студентов в образовательном учреждении»

Мельник Нина Юрьевна, Шалаев Александр Дмитриевич.

Научный руководитель: *д.т.н., Белевитин Владимир Анатольевич.*

В сборнике IX Всероссийской научно-практической конференции «Актуальные вопросы, достижения и инновации». – Пенза, 2021.