Министерство образования и науки Челябинской области

Государственное бюджетное профессиональное образовательное учреждение

**«**Копейский политехнический колледж имени С.В.Хохрякова»

(ГБПОУ “КПК имени С.В.Хохрякова”)

Курсовая работа

УСТРОЙСТВО И ФУНКЦИОНИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМА “ПОРТАЛ ГОСУДАРСВТННЫХ УСЛУГ”

Руководитель

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Абдулвалеева З.В.

Выполнил

обучающийся гр. 1-ИСиП-18

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Давлетов Д.Н.

Копейск 2021

|  |
| --- |
| КУРСОВАЯ РАБОТА  по МДК.07.01  УСТРОЙСТВО И ФУНКЦИОНИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМ  ДАВЛЕТОВ ДАНИИЛ НИКОЛАЕВИЧ  Копейск 2021 |

Оглавление

Изм.

Лист

№ докум.

Подпись

Дата

Лист

2

Разраб.

Давлетов Д.Д

Пров.

Абдулвалеева З.В

Лит.

Листов

35

Гр. 1ИСиП-18

|  |
| --- |
| Введение ...................................................................................................................4 |
| 1. Характеристика состава автоматизированной системы...................................5  2. Программная и эксплуатационная документация…...………………….….....6 |
| 3. Установка и настройка SQL - Сервера……………………………………..….8 |
| 4. Проектирование и структуры базы данных…………………………........... ..9 |
| 5. Работа с журналом аудита базы данных. Мониторинг нагрузки сервера... .11 |
| 6. Настройки политики безопасности .............................................................. ...13 |
| 7. Обеспечение восстановления базы данных.....................................................16 |
| Заключение……………………………………………….………………………..40  Библиография |

Введение.

Лист

3

Информационная система (ИС) – это организационно упорядоченная взаимосвязанная совокупность средств, и методов информационных технологий, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели. Такое понимание информационной системы предполагает использование в качестве основного технического средства переработки информации ЭВМ и средств связи, реализующих информационные процессы и выдачу информации, необходимой в процессе принятия решений задач из любой области.

ИС является средой, составляющими элементами которой являются компьютеры, компьютерные сети, программные продукты, базы данных, люди, различного рода технические и программные средства связи и т.д. Хотя сама идея ИС и некоторые принципы ее организации возникли задолго до появления компьютеров, однако компьютеризация в десятки и сотни раз повысила эффективность ИС и расширила сферы их применения.

1.Харакетристика состава автоматизированной системы

Лист

4

Автоматизированная информационная система (Automated information system, AIS) - это совокупность программных и аппаратных средств, предназначенных для хранения и (или) управления данными и информацией, а также для производства вычислений.

Основная цель АИС – хранение, обеспечение эффективного поиска и передачи информации по соответствующим запросам для наиболее полного удовлетворения информационных запросов большого числа пользователей.

К основным принципам автоматизации информационных процессов относят: окупаемость, надежность, гибкость, безопасность, дружественность, соответствие стандартам.

Окупаемость означает затрату меньших средств, на получение эффективной, надёжной, производительной системы, возможностью быстрого решения поставленных задач.

• Надежность достигается использованием надёжных программных и технических средств, использования современных технологий.

• Гибкость означает легкую адаптацию системы к изменению требований к ней, к вводимым новым функциям. Это обычно достигается созданием модульной системы.

• Безопасность означает обеспечение сохранности информации, регламентация работы с системой, использование специального оборудования и шифров.

• Дружественность заключается в том, что система должна быть простой, удобной для освоения и использования (меню, подсказки, система исправления ошибок и др.).

Выделяются четыре типа АИС:

Лист

5

1. Охватывающий один процесс (операцию) в одной организации.

2. Объединяющий несколько процессов в одной организации.

3. Обеспечивающий функционирование одного процесса в масштабе нескольких взаимодействующих организаций.

Реализующий работу нескольких процессов или систем в масштабе нескольких организаций.

АИС можно представить, как комплекс автоматизированных информационных технологий, составляющих информационную систему, предназначенную для информационного обслуживания потребителей.

Основное назначение автоматизированных информационных систем не просто собрать и сохранить электронные информационные ресурсы, но и обеспечить к ним доступ пользователей. Одной из важнейших особенностей АИС является организация поиска данных в их информационных массивах (базах данных). Поэтому АИС практически являются автоматизированными информационно-поисковыми системами (АИПС)

Автоматизированная информационно-поисковая система - программный продукт, предназначенный для реализации процессов ввода, обработки, хранения, поиска, представления данных т.п.

• АИПС бывают фактографическими и документальными.

• Фактографические АИПС обычно используют табличные реляционные БД с фиксированной структурой данных (записей).

• Документальные АИПС отличаются неопределённостью или переменной структурой данных (документов). Для их разработки обычно применяются оболочки АИС.

В качестве предметной области выбрано образовательное учреждение «Автошкола», которое занимается обучением вождению транспортных средств. Информационная система (ИС) данного образовательного учреждения занимается подготовкой к обучению, сдачи экзаменов.

Для осуществления работы автошколы между преподавателем, инструктором и учеником необходима следующая информация:

Лист

6

Персональные данные преподавателя;

Персональные данные инструктора;

Персональные и контактные данные ученика.

Информация, хранящаяся в разрабатываемой системе, не будет носить строго конфиденциального характера и для обеспечения функционирования программы "Автошкола" произведено разграничение прав доступа с помощью пароля. После ввода пароля разрешается доступ к базе данных, а без ввода пароля база данных не доступна. Таким образом, необходимо реализовать ввод, хранение и изменение информации в базе данных:

Персональные и контактные данные ученика (ФИО, группа, паспортные данные, ИНН, адрес, телефон);

Персональные и контактные данные преподавателя (ФИО, возраст, образование, стаж, телефон);

Персональные и контактные данные инструктора (ФИО, возраст, образование, стаж, телефон).

Данные по группам (название).

Также предусматриваются выходные данные:

Табель посещения;

Состав группы;

Отчет об оплате за посещение;

Список преподавателей;

Список инструкторов;

Список учеников.

Конечный продукт должен выполнять следующие функции:

Ввод, изменение и удаление данных во всех таблицах;

Печать списка инструкторов;

Печать списка группы: преподаватель и ученики;

Лист

7

Печать карточки ученика: вся имеющаяся информация;

Для реализации вышеперечисленных функций конечный продукт должен содержать следующие формы:

Главную (начальную) форму выбора действий, из которых должны запускаться остальные формы, реализующие все функции;

Форма редактирования группы, сопряженная с выбором преподавателя и ученика;

Форма редактирования ученика, сопряженная с выбором инструктора;

Форма редактирования табеля посещения и оплаты, сопряженная с выбором ученика и группы.

Автошкола выполняет следующие задачи:

Ведет учет учеников, их количество и посещаемость в разных группах.

Ведет учёт договоров учеников с автошколой.

Ведет учет по оплате обучения учениками.

Составляет расписание, согласует время занятий и обеспечивает явку преподавателей.

Привязывает к определенному ученику определенного инструктора.

Оформляет списки выпускников для дальнейшей сдачи экзамена в государственной инспекции безопасности дорожного движения.

Формирует учебную литературу для обеспечения учебного процесса в автошколе.

Обеспечивает выполнение требований государственного стандарта для автодрома, а также своевременную уборку и наличие конусов.

Выдаёт сертификат об окончании обучения.

Предоставляет различную справочную информацию.

2. Программная и эксплуатационная документация

Лист

8

Требования к программному обеспечению:

ОС: Windows 7 or 10.

Процессор: 2ух ядерный, частота 1.7 Ггц.

Оперативная память: 4 GB ОЗУ

Место на диске: 500 MB.

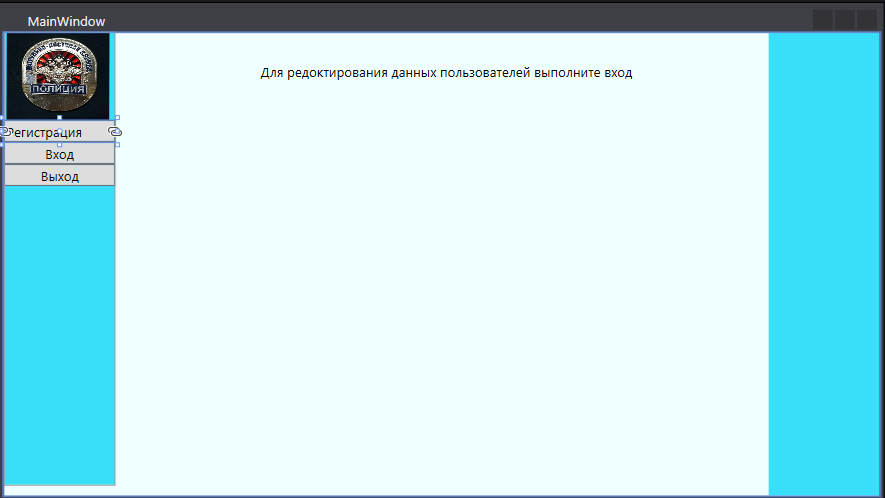
Установка:

Установка приложения выполняется с диска или по ссылке в интернете.

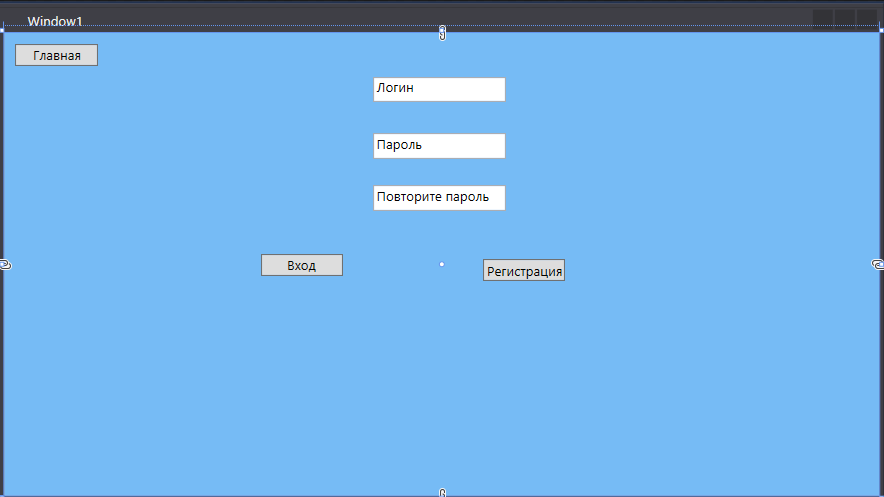
Запуск приложения:

Для запуска приложения необходимо два раза нажать на ярлык самого приложения, далее нужно подождать пару секунд и приложение откроется.

Интерфейс приложения:

При запуске приложения появляется главное окно, где можно увидеть три кнопки «Вход», «Регистрация», «Выход».

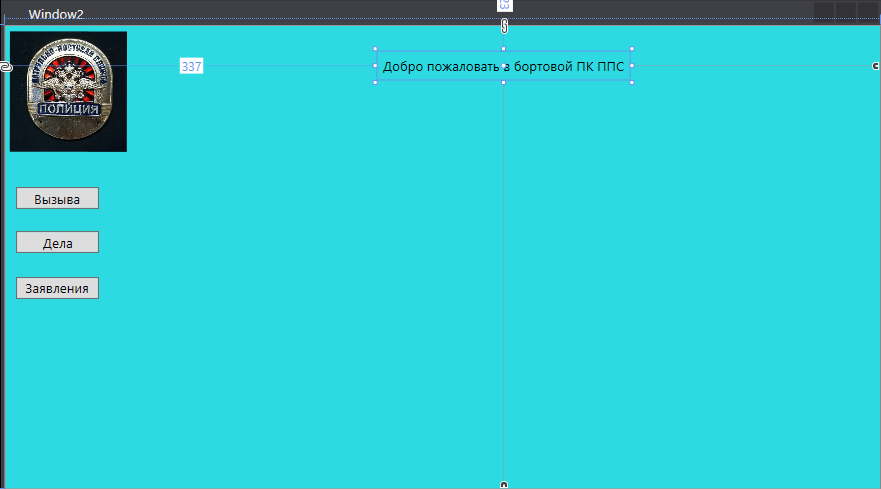
Для использования приложения необходимо зарегистрироваться, перейдя в окно регистрации вводим свои данные и, если регистрация прошла успешно далее выполняем вход.



Лист

8

После авторизации пользователь попадает в личный кабинет, где должен заполнить свои личные данные, чтобы использовать весь функционал приложения.



После того как пользователь ввёл свои данные он может использовать функционал бортового ПК, просматривать вызова и заполнять заявление от граждан.

Лист

8

3.Установка и настройка SQL сервера

Лист

9

Первое, что нужно сделать - это скачать сам дистрибутив. Скачать его можно с официального сайта.

Необходимо открыть дистрибутив и запустить установку. В меню слева нужно нажать "Installation" => New SQL Server stand-alone installation.

В новом открывшемся окне вас запросят выбрать бесплатную версию установки, к примеру "Ознакомительныя", то есть Evaluation, либо если у вас есть ключ активации, для SQL Server, или любой другой полнофункциональный ключ, то вводите его.

Приобрести ключ активации SQL Server можно на официальном сайте программы.

Читаем и соглашаемся с лицензионным соглашением.

Соглашаемся на загрузку обновлений при наличии доступа в интернет. (либо можете отказаться, тут опционально).

В следующем окне нам предлагают выбрать компоненты MS SQL Server, которые Вы хотите установить. Выбираете нужные компоненты под Ваши задачи и идем далее.

Теперь нужно установить экземпляр. Если на вашем сервере, или виртуальной машине еще не установлен никакой SQL Server, то можете выбрать "Default instance", если уже SQL Server был установлен ранее и вы поверх его ставите еще один экземпляр, то Вам нужно выбрать "Named instance" и дать ему имя.

В следующем окне нам предлагают выбрать сервисные аккаунты, это те учетные записи из-под которых будут стартовать службы SQL Server Agent, SQL Server Database, SQL Server Browser. По умолчанию используются персонализированные учетные записи.

Лист

8

Но вы можете выбрать учетную запись Вашего домена, если Ваша сеть работает на домене (сервер включен в домен).

Не забываем выбрать то, как будут стартовать службы, автоматически, вручную, либо вообще будут отключены, если они не нужны под Ваши задачи.

 Следующим пунктом нам предлагают выбрать серверную конфигурацию. Здесь предлагают выбрать, что вы сможете подключиться только с Windows логинами к SQL Серверу, либо Mixed, что вы сможете еще подключиться внутренними учетными записями SQL Server, создав их в SQL Server.

После на данном этапе имеет смысл нажать кнопку "Add Current User" и добавить текущего пользователя, а также Вы можете добавить учетную запись Вашего домена.

В том же окне переходим во вкладку "Data Directories". В этом пункте Вы можете выбрать Root директорию, директорию куда будут по умолчанию создаваться базы данных, директорию лог файлов и директорию для бекапов. Соответственно желательно, чтобы все директории были на разных жестких дисках.

В следующей вкладке переходим к настройкам базы TempDB. Это системная база, которая используется для хранения временных объектов.

Количество файлов прописано по умолчанию от кол-ва ядер.

Инициализиционный размер в мегабайтах - здесь имеет смысл прибавить размер хотя бы до 16, или 32 мб.

Autogrowth MB - Это то кол-во мегабайт, которое будет приращиваться, если файл будет заполнен на 100%. Выбираем на свое усмотрение, в зависимости от Ваших задач и размер БД, по умолчанию средний размер 64мб, но лучше, чтобы было не более 1гб, дабы не страдала производительность. Если не знаете какая будет нагрузка на Вашу базу, то оставьте как есть.

Лист

10

Лист

11

Директория для временных файлов в идеале должна быть отдельным диском.

Следующая вкладка — это настройки Filestream - это настройка, которая позволяет хранить файлы в файловой системе NTFS, она может быть, как активирована, так и нет, опционально.

В разделе Ready to Install Вы можете наблюдать все те настройки, которые ранее прописали.

Нажимаем Next и ждем пока все установится.

Если все установилось успешно, то в конце все компоненты будут "Succeeded".

4.Проектирование структуры БД

Лист

12

Проектирование программного обеспечения — процесс создания проекта программного обеспечения (ПО), а также дисциплина, изучающая методы проектирования. Проектирование ПО является частным случаем проектирования продуктов и процессов.

Целью проектирования является определение внутренних свойств системы и детализации её внешних (видимых) свойств на основе выданных заказчиком требований к ПО (исходные условия задачи). Эти требования подвергаются анализу.

Проектирование ПО включает следующие основные виды деятельности:

выбор метода и стратегии решения;

выбор представления внутренних данных;

разработка основного алгоритма;

документирование ПО;

тестирование и подбор тестов;

выбор представления входных данных.

Первоначально программа рассматривается как чёрный ящик. Ход процесса проектирования и его результаты зависят не только от состава требований, но и выбранной модели процесса, опыта проектировщика.

Модель предметной области накладывает ограничения на бизнес-логику и структуры данных.

В зависимости от класса, создаваемого ПО, процесс проектирования может обеспечиваться как «ручным» проектированием, так и различными средствами его автоматизации. В процессе проектирования ПО для выражения его характеристик используются различные нотации — блок-схемы, ER-диаграммы, UML-диаграммы, DFD-диаграммы, а также макеты.

Лист

13

Проектированию обычно подлежат:

Архитектура ПО;

Устройство компонентов ПО;

База данных «Автошкола» состоит из 8 таблиц:

1.Автомобили

2.Группы

3.Категории

4.Пользователи

5.Программа обучения

6.Тип коробки передач

7.Учебные классы

8.Занятия

Также в данных таблицах существуют столбцы:

1.Автомобили (Наименование, Гос. Номер, Категория, Тип коробки передач, Инструктор)

2.Группы (Наименование)

3.Категории (Наименование)

4.Пользователи (Логин, Пароль, id)

5.Программа обучения (Наименование, Стоимость, Категории, Количество часов теории, Количество теории практики)

6.Тип коробки передач (Наименование, Наименование автомобиля)

7.Учебные классы (Наименование, Адрес)

8.Занятия (Дата и время, Вид занятия, Инструктор, Преподаватель)

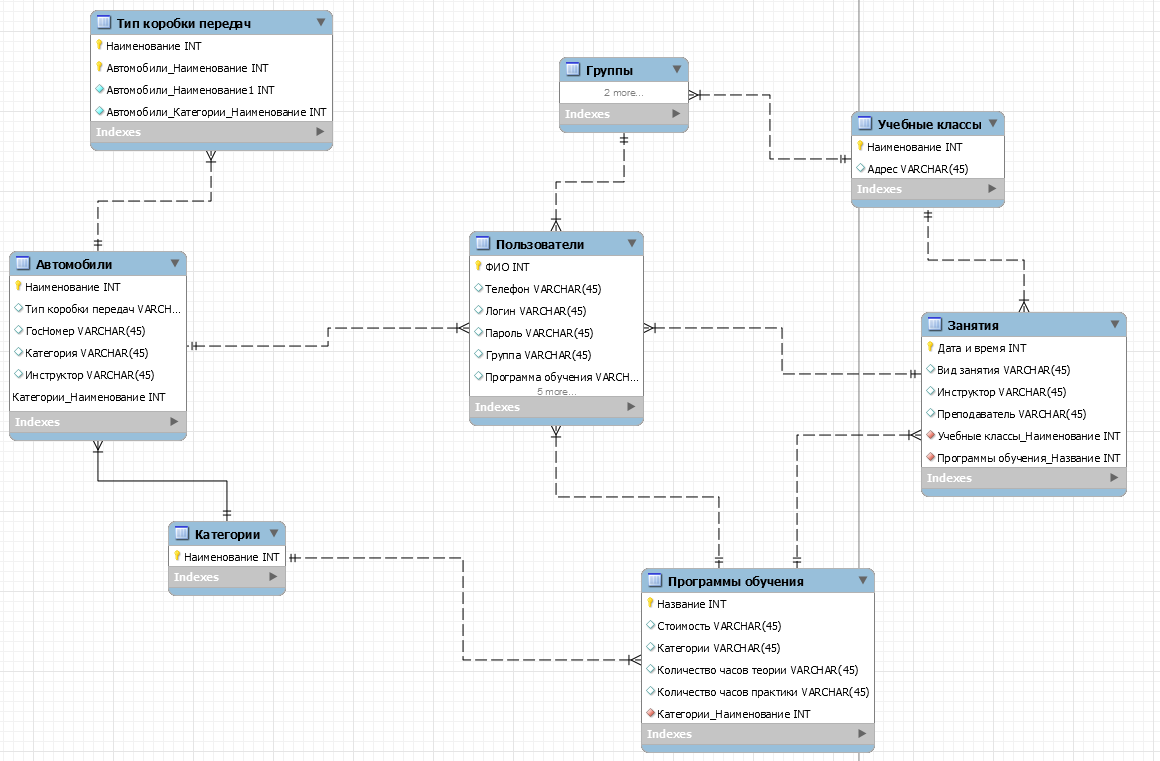
Лист

14

Также модель БД представлена и в виде ER-Диаграммы.

ER -модель представляет собой схему, составными элементами которой являются: Сущность — это реальный, либо воображаемый объект,

информацию о котором необходимо хранить в базе данных. На диаграмме ER-модели сущность изображается в виде прямоугольника, содержащего имя сущности.



5.Работа с журналом аудита БД. Мониторинг нагрузки сервера.

Лист

8

Аудит баз данных

Иногда необходимо регистрировать информацию об операциях, выполняемых в системе баз данных. Это насыпается аудитом (***audit***). Например, может потребоваться статистика о том, какие действия в системе выполняют пользователи. Аудит можно применять также для слежения за базой данных с целью обнаружения потенциальных нарушении ее защиты.

Избирательный аудит

Средство аудита SQL можно включать и выключать. При включении аудита требуется определенный расход ресурсов, необходимый для гене­рации записей аудита. Чтобы свести к минимумуработу, выполняемую SQL для аудита базы данных, нужно точно определить, для чего нужен аудит:

* Можно выполнять аудит конкретных SQL-операторов безотноси­тельно к конкретным объектам. Например, можно просить SQL генерировать запись аудита всякий раз, когда какой-либо пользователь выполняет оператор DROPTABLE, и не учитывать, к какой таблице относится этот оператор.
* Можно выполнять аудит использования мощных системных привилегий. Например, просить SQL генерировать запись аудита всякий раз, когда какой-либо пользователь применяет системную привилегию SELECTANYTABLE для запроса к таблице базы данных.
* Можно выполнять аудит определенных SQL-операторов для конкретных объектов базы данных. Например, просить SQL генерировать запись аудита всякий раз, когда какой-либо пользователь удаляет запись из таблицы SALES.CUSTOMERS.
* Для каждой разрешенной опции аудита можно просить SQL генерировать запись аудита для успешного, неуспешного или любого выполнения операторов. Более того, можно установить каждую разрешенную опцию аудита для всех либо для некоторых пользователей базы данных.

Лист

8

Записи аудита и журнал аудита

SQL генерирует записи аудита только после того, как аудит разрешен и для него установлены соответствующие опции. Например, можно установить опции аудита для конкретных операторов, объектов и пользователей. В каждую запись аудита включается информация о контролируемом операторе: какая операция выполнялась, какой пользователь ее выполнял, а также дата и время ее выполнения.

SQL хранит сгенерированные записи аудита в журнале аудита (***audittrail***), называемом также контрольным журналом. Журнал аудита — это место хранения информации аудита. В SQL разрешается сохранять генерируемые записи аудита либо в журнале аудита базы данных, либо в таком же журнале операционной системы, в которой работает SQLServer. При использовании журнала аудита базы данных можно легко просматривать и находить записи аудита с помощью SQL-запросов и предварительно созданных для этого журнала представлений словаря данных. При использовании журнала аудита операционной системы можно объединять информацию аудита базы данных с информацией аудита операционной системы.

Мониторинг - это плановое наблюдение в режиме реального времени за сервером на предопределенных условиях, например, сколько времени занимает удачное выполнение важного приложения, сколько времени занимает резервное копирование или, когда определенные значения производительности будут достигнуты. Мониторинг позволяет определить, какое событие вывело ошибку на монитор, установить, кто получает

извещения о событиях и автоматически послать извещение, когда появляется событие с ошибкой.

Использование вычислительных ресурсов отражается занятостью ресурсов центрального процессора, оперативной, внешней и виртуальной памяти, каналов ввода-вывода, терминалов и каналов связи в виде абсолютной занятости ресурсов различных видов либо относительной величины использования ресурсов каждого вида.

Информация о поведении системы должна накапливаться в результате постоянного мониторинга работы БД. Эта информация позволяет выполнять статистический анализ с целью локализации возникающих отклонений. Должен проводиться мониторинг контроля соответствия эксплуатационных параметров допустимым интервалам, лежащим между заданными пороговыми значениями. При этом положение центральной точки интервала допустимых значений может задаваться «базовой» функцией или быть константой. При выходе контролируемых параметров за пределы допустимых значений система мониторинга должна извещать персонал о возникших отклонениях. Администратор определяет для каждого хоста, какое событие заслуживает внимания (к примеру, слишком высокая нагрузка) и какая реакция должна последовать. Кроме того, в случае возникновения проблемы процесс может отправлять сообщение ответственному сотруднику по электронной почте с помощью службы немедленного обмена сообщениями или в виде SMS. Возможна также установка обработчика событий — программы, которая запускается при появлении ошибок. Если, к примеру, устанавливается, что Web-сервер больше не доступен, то система мониторинга должна самостоятельно перезапустить его.

Лист

8

6.Настройки политики безопасности

Лист

8

Информационная безопасность -- это состояние защищённости информационной среды. Сама же защита информации представляет собой деятельность для предотвращения утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

В то время, информационная безопасность организации -- состояние защищённости информационной среды организации, обеспечивающее её формирование, использование и развитие.

На данный момент для большинства организаций политика безопасности абсолютно необходима. В первую очередь она определяет отношение организации к обеспечению безопасности и необходимые действия организации по защите своих ресурсов и данных. На основе политики безопасности устанавливаются необходимые средства и процедуры для обеспечения безопасности, а также определяются роли и ответственность сотрудников организации в обеспечении безопасности.

Политика безопасности организации включает:

* Базовую политику безопасности;
* Специализированные политики безопасности;
* Процедуру безопасности.

Базовая политика безопасности

Лист

8

Под базовой политикой безопасности понимается, как организация обрабатывает информацию, кто может получить к ней доступ и каким способом. Подход, реализуемый базовой политикой безопасности, дает возможность постепенно и последовательно выполнять работу по созданию системы безопасности, не пытаясь сразу выполнить ее целиком. Базовая политика является основной для организации или предприятия. В свою очередь, она определяет:

* Ценность технологических и информационных активов организации;
* Риск потери, либо повреждения данных активов;
* Уровень безопасности, определяющий защиту каждого актива, то есть мер безопасности, которые можно считать рентабельными для применения;
* Политику безопасности организации на базе предыдущих этапов;
* Необходимость финансовых ресурсов для реализации политики безопасности, приобретение и установки требуемых средств безопасности;
* Необходимость проведения разъяснительных мероприятий и обучения персонала для поддержки сотрудниками и руководством требуемых мер безопасности;
* Надобность проведения регулярного контроля безопасности с целью выявления текущих проблем, учета изменения внешнего окружения и внесение необходимых изменений в состав персонала.

Специализированные политики безопасности

Лист

8

Существуют десятки специализированных политик, которые могут применяться большинством организаций среднего и большого размера. Некоторые из них предназначены для любой организации, другие -- специфичны для определенных окружений.

С учетом особенностей применения специализированные политики безопасности можно разделить на две группы:

\* политики, затрагивающие значительное число пользователей;

\* политики, связанные с конкретными техническими областями.

К специализированным политикам, затрагивающим значительное число пользователей, относятся:

* политика допустимого использования;
* политика удаленного доступа к ресурсам сети;
* политика защиты информации;
* политика защиты паролей и др.

Политика допустимого использования

Цель данной политики -- установление стандартных норм безопасного использования компьютерного оборудования и сервисов в компании, а также соответствующих мер безопасности сотрудников для защиты корпоративных данных и собственной информации. Неправильное использование компьютерного оборудования и сервисов подвергает компанию рискам, включая вирусные атаки, DDOS атаки, нарушение сетевых систем и сервисов, а самое главное потерю конфиденциальных данных компании. Политика допустимого использования применяется к сотрудникам, консультантам, временным служащим и другим работникам компании, включая сотрудников сторонних организаций. Политика допустимого использования предназначена в основном для конечных пользователей и указывает им, какие действия разрешаются, а какие запрещены. Политика допустимого использования устанавливает:

* ответственность пользователей за защиту любой информации, используемой и/или хранимой их компьютерами;

Лист

8

* правомочность пользователей читать и копировать файлы, которые не являются их собственными, но доступны им;
* уровень допустимого использования электронной почты и Web-доступа.
* Разработка такой политики выполняется квалифицированными специалистами организации по соответствующему сервису, системе или подсистеме под контролем комиссии (команды), которой поручена разработка политики безопасности организации.

Политика удаленного доступа

Ее цель -- установление стандартных норм безопасного удаленного соединения любого хоста с сетью компании. Стандартные нормы призваны минимизировать ущерб компании из-за возможного неавторизованного использования ресурсов компании. К такому ущербу относятся: утрата интеллектуальной собственности компании, потеря конфиденциальных данных, искажение имиджа компании, повреждения критических внутренних систем компании.

Эта политика касается всех сотрудников, поставщиков и агентов компании при использовании ими для удаленного соединения с сетью компании компьютеров или рабочих станций, являющихся собственностью компании или находящихся в личной собственности.

Политика удаленного доступа:

* Намечает и определяет допустимые методы удаленного соединения с внутренней сетью;
* Существенна в большой организации, где сети территориально распределены;
* Должна охватывать по возможности все распространенные методы удаленного доступа к внутренним ресурсам.

Лист

8

* Политика удаленного доступа определяет:
* Какие методы разрешаются для удаленного доступа;
* Ограничения на данные, к которым можно получить удаленный доступ;
* Кто из пользователей может иметь удаленный доступ

Защищенный удаленный доступ должен быть строго контролируемым. Применяемая процедура контроля должна гарантировать, что доступ к информации организации или сервисам получат только прошедшие проверку люди. Сотрудник компании не должен передавать свой логин и пароль никогда и никому, включая членов семьи. Управление удаленным доступом не должно быть сложным и приводить к возникновению ошибок. Контроль доступа целесообразно выполнять с помощью одноразовой парольной аутентификации или с помощью открытых/секретных ключей. Сотрудники компании с правами удаленного доступа должны гарантировать, что принадлежащие им или компании персональный компьютер или рабочая станция, которые удаленно подсоединены к корпоративной сети компании, не будут связаны в это же время с какой-либо другой сетью, за исключением персональных сетей, находящихся под полным контролем пользователя. Кроме того, их соединение удаленного доступа должно иметь такие же характеристики безопасности, как обычное локальное соединение с компанией. Все пользователи, которые подключены к внутренним сетям компании с помощью технологий удаленного доступа, должны использовать самое современное антивирусное обеспечение.

Процедуры безопасности

Для любой организации процедуры безопасности являются необходимым и важным дополнением к политикам безопасности. Поскольку политики безопасности только описывают, что должно быть защищено и каковы основные правила защиты, то процедуры безопасности определяют, как защитить ресурсы и каковы механизмы исполнения политики, другими словами, как реализовать политику безопасности.

Процедуры безопасности:

Многие процедуры, связанные с безопасностью, должны быть стандартными средствами в любом подразделении. Существуют несколько важных процедур безопасности, которые необходимы почти каждой организации.

Лист

8

Первая из них - это процедура реагирования на события. Она является необходимым средством безопасности для большинства организаций. Организация особенно уязвима, когда обнаруживается вторжение в ее сеть или, когда она сталкивается со стихийным бедствием.

Процедур реагирования на события иногда называют процедурой обработки событий или процедурой реагирования на инциденты. Практически невозможно указать отклики на все события нарушений безопасности, но нужно стремиться охватить основные типы нарушений, которые могут произойти. Например: сканирование портов сети, атака типа "отказ в обслуживании", компрометация хоста, НСД и др. Данная процедура определяет: \* обязанности членов команды реагирования; \* какую информацию регистрировать и прослеживать; \* как обрабатывать исследование отклонений от нормы и атаки вторжения; \* кого и когда уведомлять; \* кто может выпускать в свет информацию и какова процедура выпуска информации; \* как должен выполняться последующий анализ и кто будет в этом участвовать.

7. Обеспечение восстановления базы данных.

Лист

8

Заключение

Лист

34

С развитием информационных технологий возросла необходимость в защите данных. Многие способы защиты информации, актуальные несколько лет назад, устарели. Биометрические системы защиты еще набирают популярность и востребованность. У таких систем есть будущее, поэтому считаю, что информационная система “Портал государственных услуг” найдет место в информационных системах, требующих высокую степень защиты и надежности.

По окончании курсовой работы была описана информационная система “Портал государственных услуг”. Были приведены некоторые требования к данной системе, описана документация и техническое задание.

В ходе работы также были выявлены недостатки системы, которые будут анализированы и устранены в последующих версиях. Будут добавлены и новые функции. Таким образом, информационная система “Портал государственных услуг” усовершенствоваться и модернизироваться.

Лист

35

Список использованных источников

1. ГОСТ 2.105-95. Единая система конструкторской документации. Общие требования к текстовым документам. - Введен в действие постановлением Госстандарта РФ от 8 августа 1995 г. №426.

2. ГОСТ 7.80-2000. Библиографическая запись. Заголовок. Общие требования и правила составления. - Введение. 2000-01-07. - М.: Изд-во стандартов, 2000. - (Система стандартов по информации, библиотечному и издательскому делу).

3. ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

4. Васильков А. В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. - М.: Форум, 2015.

5. Гвоздева В. А. Информатика, автоматизированные информационные технологии и системы / В.А. Гвоздева. - М.: Форум, Инфра-М, 2017. - 544 c.

6. Голицына, Максимов, Попов: Информационные системы. Учебное пособие

7. Ивлев В. А. Информационные системы на основе действий / В.А. Ивлев, Т.В. Попова. - М.: 1С-Паблишинг, 2017.

8. Исаев Г.Н., Роганов А.А. Управление информационными системами. (Бакалавриат). Учебное пособие.

9. Киселев Г. М. Информационные технологии в педагогическом образовании // Бочкова Р.В. – 2014 – С.

10. Троелсен Э., Джепикс Ф. - Язык программирования C# 7 и платформы .NET и .NET Core – 2018.

11. Черников, Б. В. Информационные технологии управления / Б.В. Черников. - М.: Инфра-М, Форум, 2017.

12. Абрамян, Михаил Visual C# на примерах / Михаил Абрамян. - М.: БХВ-Петербург, 2016.

Лист

36

13. Культин, Никита Основы программирования в Microsoft Visual C# 2010 / Никита Культин. - М.: БХВ-Петербург, 2017. – 389 c.

14.<https://sites.google.com/site/prikinfo16/razdel-1-informacionnye-sistemy-v-obrazovanii/tema-1-informacionnye-sistemy-i-tehnologii>

15. <https://cde.osu.ru/courses2/course157/text/1.5.html>

16. <https://metanit.com/sharp/tutorial/>

17. <https://docs.microsoft.com/ru-ru/dotnet/csharp/>