

# Теория

---

- В современном обществе стали популярными услуги по обучению вождению. Такие услуги пользуются спросом в любое время года и в любом городе. Уметь водить автомобиль и иметь отменные навыки вождения считается для современного человека обязательным умением, позволяющим быть мобильным.
- Для улучшения и совершенствования внутреннего порядка такой организации необходимо учитывать многие факторы и показатели.
- Если посмотреть поверхностно на организацию работы автошколы, то зачастую возникает проблема организационного характера, включающая в себя многие факторы.
- Из-за большого спроса на обучения возникает проблема с нехваткой современно оснащенных автомобилей, квалифицированных автоинструкторов, специализированных автодромов - всё это тормозит ход обучения.
- Ведь для многих учеников целью является «накатать» как можно больше часов и тем самым чувствовать себя уверенным на дорогах города, а сделать это можно только при большом количестве практикумов. Так что основной задачей является оптимизировать расписание практических занятий.

# Анализ Рисков и потерь

---

# Проблемы ИБ

---

- Утечка данных от Курсантов
- Безопасность информационной базы, наличие уязвимости
- Система индефикации курсантов(сечатка глаза, рук)
- несовершенство программного обеспечения, аппаратной платформы;
- разные характеристики строения автоматизированных систем в информационном потоке;
- часть процессов функционирования систем является неполноценной;
- неточность протоколов обмена информацией и интерфейса;
- сложные условия эксплуатации и расположения информации.

# Технические средства защиты информации

Группа технических средств защиты информации совмещает аппаратные и программные средства.

Основные:

- резервное копирование и удаленное хранение наиболее важных массивов данных в компьютерной системе – на регулярной основе;
- дублирование и резервирование всех подсистем сетей, которые имеют значение для сохранности данных;
- создание возможности перераспределять ресурсы сети в случаях нарушения работоспособности отдельных элементов;
- обеспечение возможности использовать резервные системы электропитания;
- обеспечение безопасности от пожара или повреждения оборудования водой;
- установка программного обеспечения, которое обеспечивает защиту баз данных и другой информации от несанкционированного доступа.

## Защиты базы данных от несанкционированного доступа

Доступ в такие базы данных может быть ограничен.

Для этого создается специальный модуль, который является основным инструментом защиты базы данных от несанкционированного доступа и предназначен для настройки, включения и отключения системы разграничения прав доступа пользователей к базе данных.



# Решение проблем ИБ

---

- **Система разграничения прав доступа должна выполнять следующие функции:**
- блокировать доступ незарегистрированных пользователей в систему.
- С этой целью все пользователи системы должны быть зарегистрированы в списке пользователей;
- определять права пользователей в системе и ограничивать действия пользователей в соответствии с этими правами:
- права на доступ к базе данных и права на пользование рабочими станциями;



Рис.1. Структура системы защиты от несанкционированного копирования

**Подсистема внедрения управляющих механизмов** представляет собой комплекс программных средств, предназначенный для подключения внедряемого защитного кода к защищаемому программному модулю.

**Внедряемый защитный код** – это программный модуль, задача которого состоит в противодействии попыткам запуска (исполнения) нелегальной копии защищаемой программы.

**Подсистема реализации защитных функций** представляет собой программную секцию, решающую задачу распознавания легальности запуска защищаемой программы.

**Подсистема противодействия нейтрализации** защитных механизмов предназначена для борьбы с возможными попытками нейтрализации системы защиты от несанкционированного копирования и/или её дискредитации.

**Блок установки** характеристик среды отвечает за получение характеристик, идентифицирующих вычислительную среду.

**Блок сравнения** характеристик среды устанавливает факт легальности запуска защищаемой программы.

**Блок ответной реакции** реализует ответные действия системы защиты на попытки несанкционированного исполнения защищаемой программы.

# *Решение проблем ИБ*

---

# Законы

---

- **Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ**
- 152-ФЗ «О персональных данных»,
- 149-ФЗ «Об информации, информационных технологиях и о защите информации»