Курсовая работа
На тему «Обеспечение инженерно-технических средств физической защиты информации на предприятии: авто-акустического оборудования «Мото»

ПРЕЗЕНТАЦИЮ ПОДГОТОВИЛ СТУДЕНТ ГБПОУ КБТ

ГРУППЫ ИБ33-20

НИКИШОВ ВЛАДИМИР

1. Исходя из схемы помещения и специфики предприятия, которое имеет площадь не более 150 м^2, можно сделать следующие выводы:
На предприятии вряд ли больше 1-2 рабочих компьютеров.
2. Предприятие является небольшим, скорее всего оно ориентировано на более дорогие единоразовые заказы, нежели на большой поток дешевых заказов.
3. Исходя из пункта 2, можно предположить, что на предприятии обычно 3-5 сотрудников.
4. Скорее всего, данное предприятие – результат хобби единомышленников, которые в какой-то момент встретились и начали заниматься изготовлением, настройкой и тюнингом авто-акустического оборудования.
5. Исходя из пункта 2, становится ясно что персонал предприятия – люди, которые долгое время работают друг с другом, поэтому риск внутренней угрозы не такой большой.
6. Посмотрев на схему, становится ясно, что предприятие находится на конечном этаже здания, будем считать, что в здании 2 или 3 этажа.
На 1 этаже находится пост охраны с проходной, туда же выходят камеры видеонаблюдения, показания датчиков и извещателей

В самом производственном помещении находятся 5 окон и 1 окно на лестнице между этажами.

Помещение является почти идеальным прямоугольником, не считая небольшого ответвления, которое никуда не ведет и является тупиком

Для входа на предприятие используется дверь с лестницы

На предприятии производится тюнинг и настройка авто-акустического оборудования.

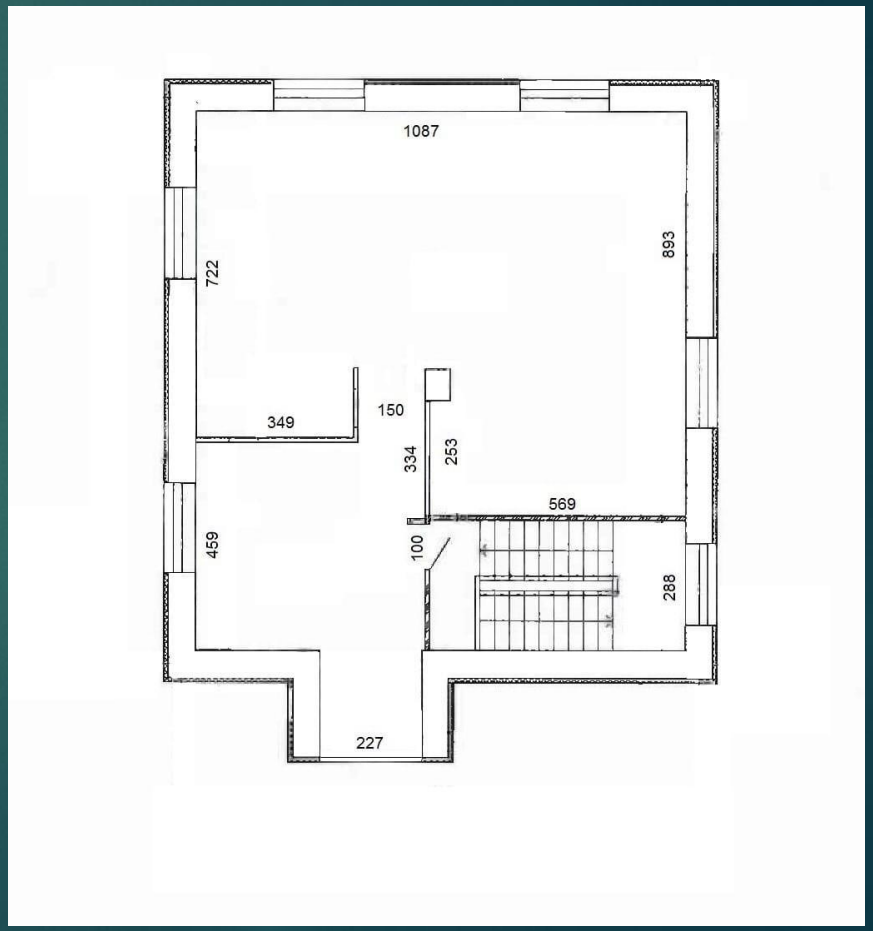
На предприятии присутствует одно рабочее место с компьютером, используемым для хранения информации о заказах, заказчиках, поставщиках и для составления финансовой отчетности.

Возможные каналы утечки информации:

- Хищение или потеря USB-накопителя.
- Подключение съемных носителей данных.
- Доступ у сотрудников к визуальной конфиденциальной информации.
- Выгрузка информации в глобальную сеть.
- Доступ к акустической конфиденциальной информации.
- Несанкционированный доступ к помещению предприятия.
- Загрузка вредоносного ПО через сеть Интернет.
- Съем информации, передаваемой по кабельным линиям связи.

Вид защищаемой информации:
Коммерческие конфиденциальные данные (2А) – информация о заказчиках, поставщиках, работниках, зарплате сотрудников, технические карты, техзадания, расходы и доходы.
Используемое ПО – 3А
Используемых каналов связи – 2А
Используемом оборудовании – 2Б

Возможные каналы утечки информации:
Хищение или потеря USB-накопителя.
Подключение съемных носителей данных.
Доступ у сотрудников к визуальной конфиденциальной информации.
Выгрузка информации в глобальную сеть.
Доступ к акустической конфиденциальной информации.
Несанкционированный доступ к помещению предприятия.
Загрузка вредоносного ПО через сеть Интернет.
Съем информации, передаваемой по кабельным линиям связи.



Анализ оборудования, которое можем использовать:

- Исходя из того, что предприятие является небольшим, для надежной защиты нам не понадобится большое количество оборудования и какие-то сильно изощренные методы и средства защиты.

Этапы защиты объекта:

- Осмотр объекта.
- Выбор оборудования для защиты.
- Проверка покрытия объекта выбранным оборудованием отталкиваясь от виртуального плана объекта.
- Установка техники и проверка работоспособности.

Для физической защиты информации нам понадобится соблюсти следующие пункты:

- Исключить доступ третьих лиц на территорию предприятия.
- Организовать видеонаблюдение за помещением.
- Защитить физические носители информации.
- Обеспечение систем оповещений о пожарной опасности.
- Обеспечение систем оповещений о проникновении.
- Обеспечение систем оповещений о изменении температуры.
- Обеспечение систем оповещений о разрушаемости объекта.

1.4 Оценка рисков

На предприятии присутствуют следующие возможные риски:

- Нарушение правил производства огневых работ -Неисправность электропроводки и электроустановок - проводка может стать таким источником только в экстремальных ситуациях, вызванных одной из причин: снижение сопротивления изоляции проводов или жил кабеля ниже критического уровня; нарушение контакта в местах соединения проводников; излом или разрыв токоведущей жилы провода или кабеля, приводящий к возникновению переходного сопротивления.
- Самовольное проникновение на охраняемое в установленном порядке предприятие.
- Несанкционированный доступ к информации — противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям.
- Неисправность оборудования – может являться причиной потери данных компаниями или частными пользователями. Злоумышленники могут вывести оборудование из строя как механическим способом, так и программным способом.
- Конфликтные ситуации среди сотрудников.
- Порча имущества фирмы.

Отталкиваясь от сформулированных ранее обязательных пунктов для защиты информации, **переходим к выбору оборудования.**

1.Исключим доступ третьих лиц с помощью укрепленной входной двери. Так же мы реализуем **СКУД** для отпирания магнитного замка с помощью специальной карты, а также установим **новую металлическую дверь**. Т.е, чтобы попасть в помещение, помимо отпирания обычного замка на двери, нужно еще отпереть магнитный замок.

2.Для организации видеонаблюдения за помещением нам будет достаточно 3-х **IP камер**, оснащенных датчиком движения.

3.Защита физических носителей информации будет производится следующим образом: требуется опечатать/опломбировать и закрыть с помощью стяжек рабочий компьютер, а также зафиксировать на месте с помощью креплений.

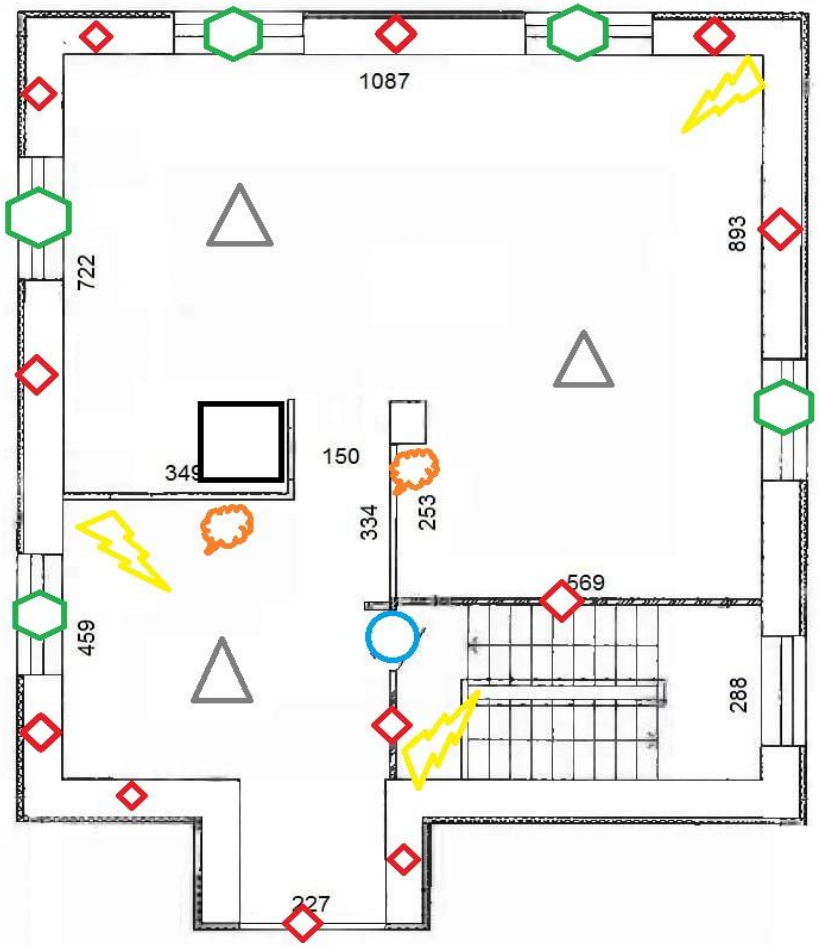
4.Обеспечение систем оповещений о пожарной опасности – установка датчиков и оповещателей, определяющих задымление и изменение температуры,

5.Обеспечение систем оповещений о изменении температуры – входят в системы оповещения о пожарной опасности. Также, в рамках пожарной безопасности требуется установка в помещении предприятия нескольких портативных огнетушителей.

6.Обеспечение систем оповещений о проникновении – установим датчики целостности на окна и стены.

7.Обеспечение систем оповещений о разрушаемости объекта – входят в системы оповещений о проникновении.

8.Определив список требуемых мер по защите, получаем следующую схему расположения систем на рассматриваемом помещении компании:



Камера

Рабочий ПК

Датчик разбития стекла

Датчик целостности

СКУД на новой двери

Огнетушитель

Комплекс пожарной защиты
(пожарный и тепловой излучатель)

СКУД

Мной выбран **СКУД с контроллером TS-CTR-Em и электромагнитным замком.**

Простая и надежная комплектация для ограничения доступа. Контроллер способен хранить в памяти до 1000 пользователей (кодовые комбинации и **RFID** карты/брелоки). Возможность удаления утерянных идентификаторов (карт/брелоков), а алгоритм добавления/удаления прост и понятен.

Описание:

- Кодовая панель может работать в 2 режимах – автономном и сетевом с подключением к внешнему контроллеру по Wiegand-26
- Возможность удаления утерянных идентификаторов
- Управление индикацией (звуковой и цветовой)
- Простая процедура записи/удаления идентификаторов при помощи мастер-карт
- Работа в режиме «шлюз», перенос памяти идентификаторов, работы до -40 градусов

Видеонаблюдение

Для организации видеонаблюдения была выбрана миниатюрная поворотная **PTZ IP-камера 2Мп Ezviz TY2 (4 мм)** с авто слежением за объектом.

Описание:

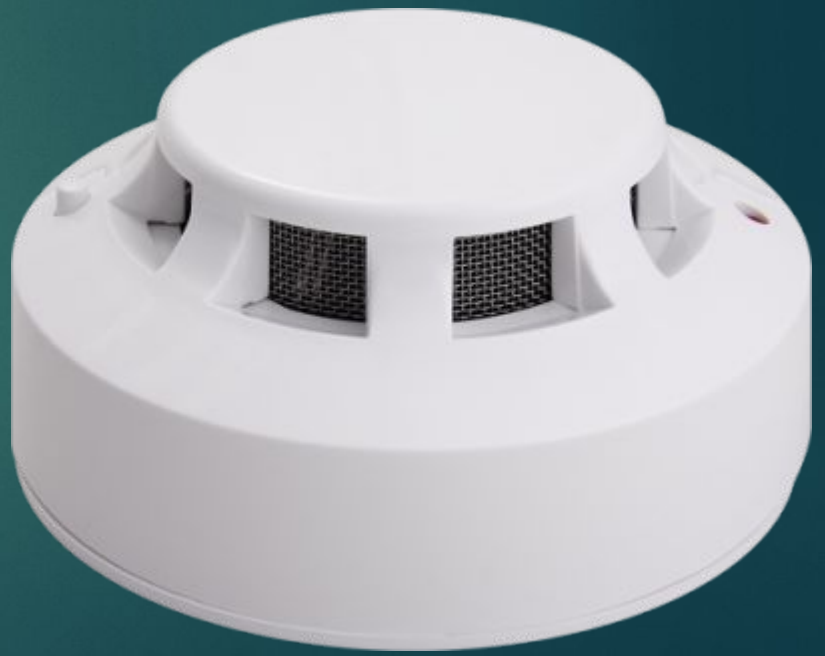
- • 1/4" CMOS матрица; объектив 4мм
- • DWDR, 3D DNR
- • Встроенный микрофон и динамик
- • Поворот по горизонтали 340°, по вертикали 120°
- • 2.4G WiFi, RJ45
- • Слежение за движением
- • Маскирование объектива
- • Поддержка microSD до 256 ГБ
- • ИК-подсветкой до 10м

Пожарная безопасность

Для обеспечения систем оповещений о пожарной опасности были выбраны **ИП212-44 с МС-01 (ДИП-44) Дымовые пожарные извещатели (4х проводные).**

Описание: Извещатель **ИП212-44 с МС-01** имеет в розетке модуль согласования **МС-01**, обеспечивающий возможность подключения извещателя в четырехпроводные шлейфы **ППК**. В модуле **МС-01** применено одноканальное оптореле с нормально-разомкнутыми контактами, которые замыкаются при срабатывании извещателя.

- Производитель: ИВС-Сигналспецавтоматика
- Тип подключения: 4х проводной
- Тип устройства: потолочный
- Способ обнаружения: дымовой
- Напряжение питания: 9-30 В
- Рабочая температура: 30…+60 °С



Пожарная безопасность

Также, для соблюдения пожарной безопасности и тушения локальных очагов возгорания был выбран **перезаряжаемый огнетушитель порошкового типа МИГ ОП- 5/з АВСЕ (2А 89В С Е) 111-07**

Описание: Огнетушитель МИГ ОП- 5/з АВСЕ (2А 89В С Е) 111-07 с повышенной огнетушащей способностью, закаченный осушенным азотом. Срок службы 15 лет. Уровень зашиты от коррозии С2 по ISO 12944-5, климатическое исполнение О2 по ГОСТ 15150. Наличие на баллоне удобного держателя распылителя.

Системы оповещений о изменении температуры

Для обеспечения систем оповещений о изменении температуры были выбраны извещатели тепловые **ИП 101-1А-А3 с температурой срабатывания +64...+76 °С.**

Описание: пожарный тепловой максимальный извещатель служит для обнаружения признаков пожара (повышение температуры среды). Тревожное извещение формируется при достижении температуры окружающей среды порогового значения.

- Извещатели предназначены для круглосуточной работы в закрытых отапливаемых помещениях и рассчитаны на совместную работу с приемно-контрольными приборами со шлейфами постоянного или знакопеременного тока.

Системы оповещений о проникновении и разрушаемости объекта

Для обеспечения систем оповещений о проникновении и разрушаемости объекта были выбраны извещатели СКИФ В и СКИФ А

- Извещатель охранный поверхностный вибрационный «СКИФ-В» предназначен для обнаружения разрушения строительных конструкций в виде бетонных стен и перекрытий толщиной не менее 0,12 м, кирпичных стен толщиной не менее 0,15 м, деревянных конструкций толщиной материала от 20 до 40 мм, фанеры толщиной не менее 4 мм, конструкций из древесностружечных плит толщиной не менее 15 мм
- Извещатель «СКИФ-А»: обеспечивает дистанционный контроль охраняемой остекленной конструкции любой конфигурации. Максимальная рабочая дальность действия извещателя -не менее 6м. Количество рабочих частот -две. Напряжение питания извещателя - 12 В