УДК 004.3

Малиничев Д.М., к.т.н., доцент
доцент кафедры «Информационной безопасности»
Российский государственный социальный университет
Россия, г. Москва
Арбатский В.В.,
студент 5 курс, факультет «Информационных технологий»
Российский государственный социальный университет
Россия, г. Москва
Мартынов М.И.,
студент 5 курс, факультет «Информационных технологий»
Российский государственный социальный университет
Россия, г. Москва

СОЗДАНИЕ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ В ООО «СИГМА»

Аннотации: *Приведено решение создания системы видеонаблюдения в ООО «Сигма».*

Ключевые слова: *Информационная безопасность, система видеонаблюдения, видеокамера.*

Annotation: *The decision of creation CCTV system in LLC «Sigma» is resulted.*

Key words: *Information security, CCTV, video camera.*

Средства защиты информации – это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

- Программные
- Смешанные
- Организационные
- Технические

Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Например:

- Встроенные средства защиты информации
- Антивирусные программы
- Специализированные программные средства защиты информации от несанкционированного доступа
- Межсетевые экраны (брандмауэры и файрволы)
- Proxy-серверы
- VPN (виртуальная частная сеть)

Аппаратные средства – это различные по типу устройства, которые аппаратными средствами решают задачи защиты информации.

Виды аппаратных средств защиты информации:

- Специализированная сеть хранения SAN
- Дисковые хранилища
- Ленточные накопители
- Электронный ключ eToken

Организационные методы защиты информации состоят из совокупности мероприятий по подбору, проверке и инструктажу персонала; обеспечению программно-технического обслуживания; назначению лиц, ответственных за конкретное оборудование; осуществлению режима секретности; обеспечению

физической охраны объектов; оборудованию помещений металлическими дверями, решетками и т.д.

Технические (аппаратные) средства защиты информации – это различные по типу устройства (механические, электромеханические, электронные и др.), которые на уровне оборудования решают задачи информационной защиты.

Для защиты периметра информационной системы создаются:

- системы охранной и пожарной сигнализации;
- системы цифрового видеонаблюдения[1-3];
- каналы связи [4-6];
- системы контроля, управления доступом (СКУД).

В данной статье рассматриваются технические средства защиты информации, а именно системы цифрового видеонаблюдения.

Было предоставлено ТЗ (техническое задание):

Имеется помещение склада с размерами 25х12х5 (ДхШхВ) (изображено на рисунке 1).

Задача: устранение всех серых (не просматриваемых) зон с возможностью идентификации личности по распознаванию лица; просмотр главных ворот склада и идентификации государственных номерных знаков проезжающих автотранспортных средств; доступ к просмотру видеозаписей, а так же видеоизображения с камер в режиме реального времени с телефона и из любой точки мира; использование только облачного хранилища.

Прилагается план помещения:

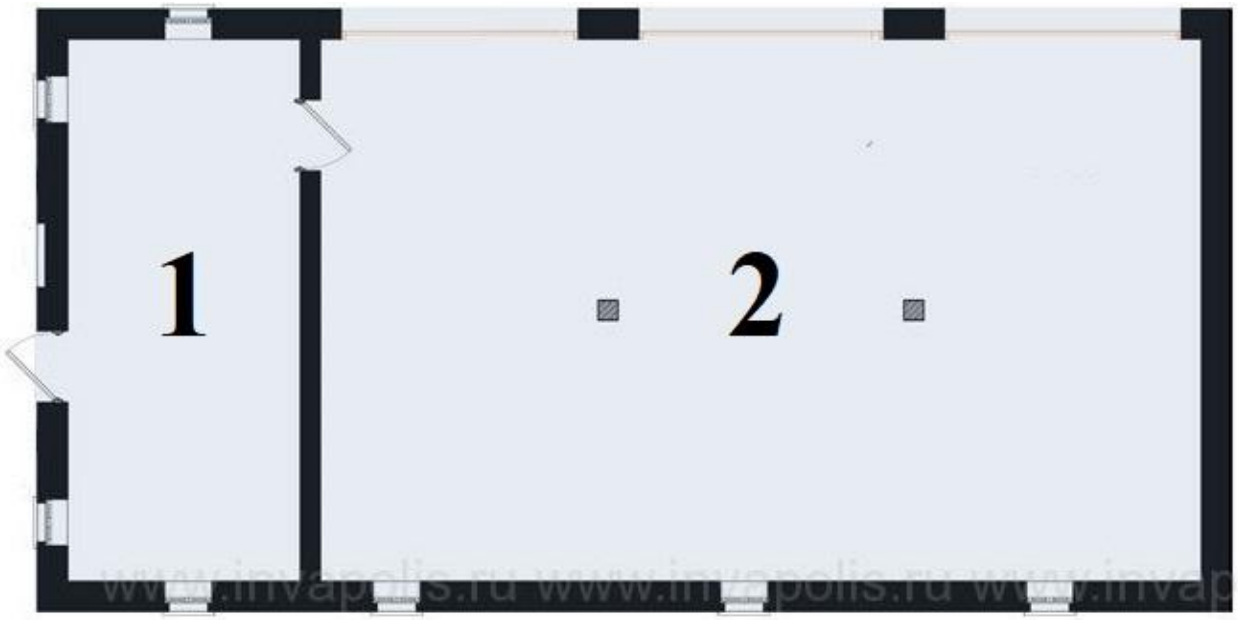

Рисунок 1. План помещения

Первое помещение имеет размеры 5,3х12 метров. Второе помещение – 19,5х12 метров. 0,2 метра – ширина перекрытия между помещениями.

В здание проведено электричество и интернет. Кабель ГВС подключен напрямую в компьютер, расположенный в первом помещении. Статический IP-адрес в глобальной сети имеется.

Совместный с заказчиком выбор остановился на камерах видеонаблюдения КАРКАМ CAM-5890P, которая имеет 5 Мп разрешение матрицы, размер матрицы 1/1.8", максимальное разрешение 2592x1944p и фреймрейт 30 к/с, подключение камеры осуществляется через разъем 10/100Mbps RJ-45, фокусное расстояние 3,6 мм.

Для работы необходимо:

1. Беспроводной маршрутизатор (любой фирмы кроме D-link и ZyXel keenetic потому что взламываются с мобильного телефона за 2-3 минуты) - 1 шт.
2. Патч-корд - 4 шт.
3. Кабель витая пара F/FTP Cat 7 - 100 метров
4. Кабель канал 20х10 2 м. - 50 шт.
5. Инжектор POE на 4 порта - 1 шт.
6. Инжектор POE на 1 порт - 4 шт.

7. Коннектор RJ-45 - 16 шт.
8. Камера IP 5Мп для внутреннего видеонаблюдения - 3 шт.
9. Камера IP 5Мп для уличного видеонаблюдения - 1 шт.

- Изначально необходимо смонтировать весь кабель канал так, как дальше будет идти кабель.
- Следующим происходит прокладка всего кабеля в кабель канал от места расположения POE-инжектора до обозначенного места расположения камер. К каждой камере должен быть проложен один провод от POE-инжектора.
- После производим монтаж внутренних камер на потолок (так мы получим большую зону обзора).
- Далее монтируем уличную камеру на высоту 4-х метров (так мы получим максимальный обзор при достаточной сохранности самой камеры)
- После окончания монтажа всех камер обжимаем каждый кабель витый пары с обоих концов коннекторами RJ-45
- Подключаем все камеры к витой паре через POE-инжектор на 1 порт: в камеру подключаем витую пару POE-инжектора и выход питающего кабеля, в POE-инжектор подключаем только что обжатый кабель витой пары
- Один из проводов, что обжаты коннекторами RJ-45, подключаем в порт «POE» POE-инжектора на 4 порта
- Подключаем беспроводной маршрутизатор и в POE-инжектор друг к другу: патч-корды одним коннектором подключаем в LAN-порт роутера, другим коннектором в LAN-порт POE-инжектора
- Подключаем кабель ГВС в WAN-порт роутера
- Подключаем маршрутизатор и POE-инжектор к розетке
- Теперь необходимо произвести настройку беспроводного маршрутизатора: подключаемся к сети данного роутера (в основном её SSID указан на нижней панели корпуса маршрутизатора и сеть открыта), открываем браузер и вводим внутренний IP-адрес маршрутизатора (который так же написан на нижней

панели корпуса). Производим быструю настройку интернет соединения в зависимости от настроек вашего провайдера. **При открытии меню с настройкой LAN сети необходимо узнать IP адреса камер. Они 192.168.0.58. Следовательно из этого, нам необходимо задать адрес роутера в сети как 192.168.0.1 для избегания конфликтов в локальной сети.**

- Подключаем POE-инжектор на 4 порта в розетку
- Во избежание конфликта IP-адресов камер необходимо изменить ее локальный IP-адрес, для этого заходим в браузер, в адресную строку вводим IP-адрес камеры, вводим логин и пароль (зачастую это admin/admin), изменяем IP-адрес на 192.168.0.101 (102,103,104 для последующих камер соответственно) и нажимаем сохранить. Так же для большей безопасности изменяет логин и пароль что были по-умолчанию. **На этом этапе так же необходимо запомнить порт устройства (в основном это 8000)**
- Подключаем все провода от камер во входы «POE» POE-инжектора по очереди и производим аналогичную настройку
- После мы имеем 4 камеры с IP-адресами 192.168.0.101, 192.168.0.102, 192.168.0.103 и 192.168.0.104 которые подключены через POE-инжектор в беспроводной маршрутизатор с IP-адресом 192.168.0.1
- Далее в настройках роутера, в разделе NAT (он так же может быть назван «преобразование сетевых адресов») добавляем правила для каждой из камер (в зависимости от марки производителя и модели маршрутизатора методы могут отличаться): прописываем внутренний IP-адрес камеры (192.168.0.101), прописываем порт (8000), прописываем свой внешний IP-адрес (узнать можно на сайте 2ip.ru) и вписываем внешний порт устройства (так же 8000). Нажимаем клавишу «включить» и «сохранить»
- После заходим на официальный сайт компании производителя камер, переходим по ссылке на представительское облачное хранилище, регистрируемся
- Теперь скачиваем из AppStore или Play Market приложение с аналогичным названием облачного хранилища и входим в ранее созданный аккаунт

- К зарегистрированному аккаунту необходимо «привязать» каждую из камер. Делается это благодаря QR-коду расположенному на коробке от камеры: на сайте нажимаем «Добавить устройство» или «+», разрешаем доступ к камере и фото галерее, сканируем QR код, вводим пароль от камеры и нажимаем «Сохранить»
- Камера отображается на главном экране программы. Все сделано верно. Повторяем это действие с каждой из камер.

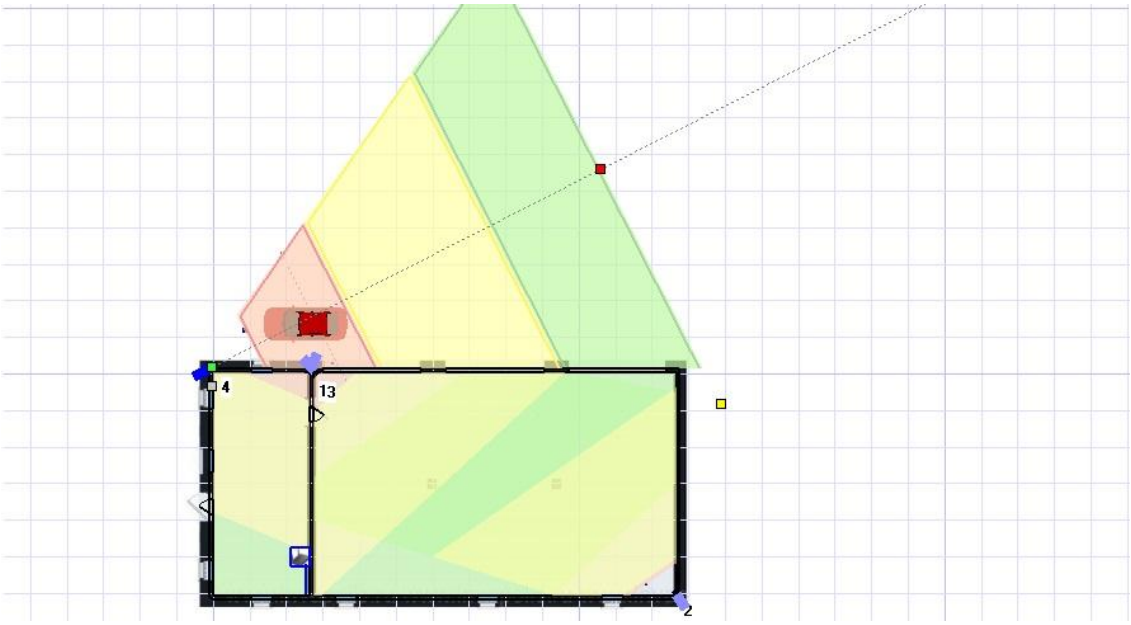

Рисунок 2. Зоны видимости камер

После всех проделанных работ имеем: устранены все серые зоны (изображено на рисунке 2), возможность идентификации личности по распознаванию лица имеется; просмотр главных ворот склада и идентификации государственных номерных знаков проезжающих автотранспортных средств имеется; возможность доступа к просмотру видеозаписей, а так же видеоизображения с камер в режиме реального времени с телефона и из любой точки мира имеется; используется только облачное хранилище, регистратор не установлен.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Герман Кругль. Профессиональное видеонаблюдение. Практика и технологии аналогового и цифрового CCTV. М. Security Focus 2011. — 640 с.
2. Пескин А.Е. Системы видеонаблюдения. Основы построения, проектирования и эксплуатации. М. Горячая линия – Телеком. 2016. — 256 с.
3. Ворона В.А., Тихонов В.А. Технические средства наблюдения в охране объектов. М. Горячая линия – Телеком. 2016. — 184 с.
4. Малиничев Д.М., Перевощиков В.А., Роткин А.М., Панфилов А.В. НЕКОТОРЫЕ ОСОБЕННОСТИ ПРИМЕНЕНИЯ В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ ШУМОПОДОБНЫХ СИГНАЛОВ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Аллея науки. 2018. Т. 1. № 9 (25). С. 944-947.
5. Малиничев Д.М., Мочалов В.В., Гусейнов Д.А. ПРИМЕНЕНИЕ ШУМОПОДОБНЫХ СИГНАЛОВ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Ежегодная международная научно-техническая конференция Системы безопасности. 2017. № 26. С. 86-87.
6. Малиничев Д.М., Бойков В.В., Болнокин В.Е. АНАЛИЗ КОРРЕЛЯЦИОННЫХ СВОЙСТВ МНОГОЗНАЧНЫХ М-ПОСЛЕДОВАТЕЛЬНОСТЕЙ Динамика сложных систем - XXI век. 2012. Т. 6. № 2. С. 83-85.