ЛЕКЦИЯ 08. УЯЗВИМОСТИ СИСТЕМ НАБЛЮДЕНИЯ, ОХРАНЫ, СИГНАЛИЗАЦИЙ

8.1. УЯЗВИМОСТИ СИСТЕМ НАБЛЮДЕНИЯ

Десятки и даже сотни тысяч систем видеонаблюдения по всему миру устроены таким образом, что получить к ним полный доступ через интернет так же легко, как прочитать вывеску на витрине супермаркета.

Обычный человек, без каких-либо навыков IT сможет подключиться к 70% систем видеонаблюдения в мире подключенных к интернет, посмотреть видео в режиме онлайн, управлять поворотными камерами, просмотреть архив, другими словами получить полный доступ к устройству видеорегистрации DVR.

Среди таких систем чаще всего можно встретить: видеонаблюдение в магазинах, гостиницах, саунах, офисах, ювелирных магазинах, банкоматах, коттеджах, квартирах, игорных заведениях, стриптиз-клубах, массажных VIP салонах.

Многие уважаемые компании по системам безопасности даже не знают этих тонкостей, некоторые ведут недобросовестно установку оборудования. Заказчики же принимают работу и радуются, но они не знают того, что в их систему может зайти любой желающий.

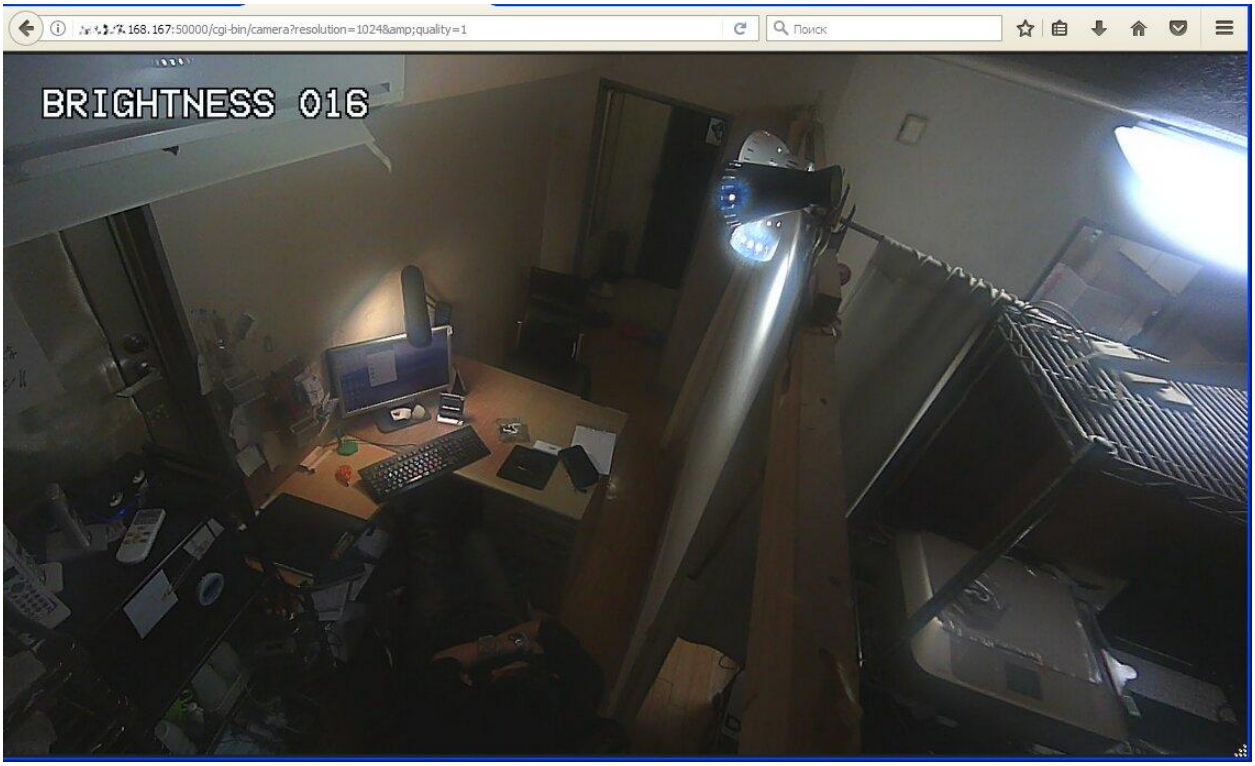
Из чего же состоит современна я система видеонаблюдения (основные элементы):

- Видеокамеры: аналоговые (с плохим качеством картинки), либо современные цифровые (HD качества);
- Микрофоны: часто можно встретить в офисах и местах, где ведется работа с клиентами.
- Видерегистратор (DVR): основа любой системы – может представлять из себя - как автономное устройство на базе linux, так и отдельный ПК с платой видеозахвата (видеосервер). На это устройство поступает сигнал с видеокамер, микрофонов, тревожных датчиков, ведется запись всей информации на HDD. К нему можно подключить монитор и мышку, управлять практически как компьютером. Так же все современные устройства DVR имеют свой LAN адаптер для подключения к сети. Вот как раз этот элемент делает возможным удаленный доступ по интернет к этому устройству.

Подключение к регистраторам из вне может осуществляться через TCP, HTTP(80), UDP и ряд некоторых других портов. Подключение через веб порт (80) поддерживают все типы DVR.

Многие люди подключают камеры в свою систему по RTSP-ссылкам. Либо чтобы сэкономить время, либо по незнанию, либо от уверенности, что так и надо, многие даже не задумываются о том, чтобы сменить пароли или посмотреть, какие настройки безопасности поддерживает их камера.

RTSP (Real Time Streaming Protocol) — это протокол, который позволяет управлять потоковым видео в режиме реального времени. Нам надо знать о нем только то, что с помощью RTSP-ссылки мы будем забирать видеопоток с камеры. У разных камер могут быть разные RTSP-ссылки, но общий вид примерно следующий: rtsp://[логин: пароль@]ip-адрес:RTSP-порт[/ключ].



8.1.1. Видеокамеры и web-камеры

IP-камеры и веб-камеры часто путают, хотя это принципиально разные устройства. Сетевая камера (видеокамера), или IP-камера, — самодостаточное средство наблюдения. Она управляется через веб-интерфейс и самостоятельно передает видеопоток по сети. По сути, это микрокомпьютер со своей ОС на базе Linux.

Сетевой интерфейс Ethernet (RJ-45) или Wi-Fi позволяет выполнять прямое подключение к IP-камере. Раньше для этого использовались фирменные клиентские приложения, но большинство современных камер управляются через браузер с любого устройства — хоть с ПК, хоть со смартфона. Как правило, IP-камеры включены постоянно и доступны удаленно. Именно этим и пользуются хакеры.

Веб-камера — пассивное устройство, которым управляют локально с компьютера (по USB) или ноутбука (если она встроенная) через драйвер операционной системы. Этот драйвер может быть двух разных типов: универсальный (предустановленный в ОС и подходящий для многих камер разных производителей) и написанный на заказ для конкретной модели.

Задача хакера здесь уже другая: не подключиться к веб-камере, а перехватить ее видеопоток, который она транслирует через драйвер. У веб-камеры нет отдельного IP-адреса и встроенного веб-сервера. Поэтому взлом веб-камеры всегда следствие взлома компьютера, к которому она подключена.

По замыслу, IP-камеру защищают от вторжения два секрета: ее IP-адрес и пароль учетной записи. На практике IP-адреса вряд ли можно назвать секретом. Они легко обнаруживаются по стандартным адресам, к тому же камеры одинаково откликаются на запросы поисковых роботов.

С паролями к камерам наблюдения дела обстоят крайне плохо. На некоторых камерах пароля просто нет, и авторизация полностью отсутствует. На других стоит заданный по умолчанию пароль, который легко найти в руководстве к камере.

Часто бывает, что производитель оставил в прошивке камеры служебный вход для сервис-центров. Он остается открытым даже после того, как владелец камеры сменил дефолтный пароль.

Любую веб-камеру можно превратить в подобие IP-камеры, если установить на подключенном к ней устройстве сервер видеонаблюдения. На компьютерах многие используют для этих целей старый webcamXP, чуть более новый webcam 7 и подобные программы.

В последнее время старые смартфоны и планшеты нередко приспосабливают для домашнего видеонаблюдения. Чаще всего на них ставят Android Webcam Server — простое приложение, которое транслирует видеопоток со встроенной камеры в интернет. Оно принимает запросы на порт 8080 и открывает панель управления на странице с говорящим названием /remote.html. Попав на нее, можно менять настройки камеры и смотреть изображение прямо в окне браузера (со звуком или без).

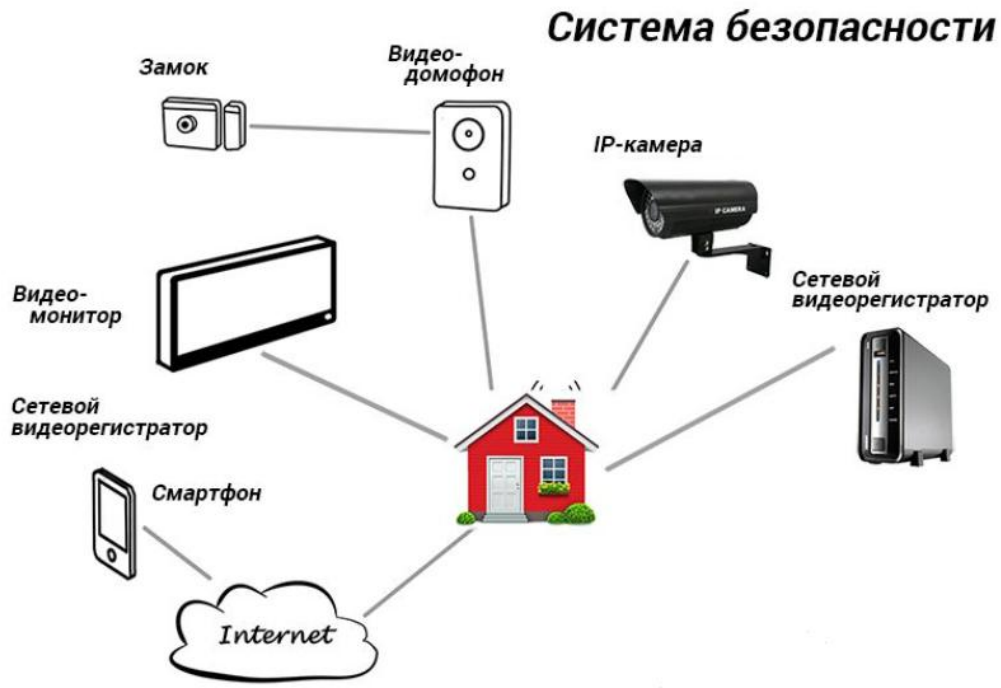
8.1.2. Защита от подмены потока с камер

1. Обновление прошивки
2. Смена стандартных логинов и паролей
3. Фильтр IP-адреса
4. Включение обязательной авторизации. Данная функция присутствует во многих современных камерах, но, к сожалению, не все пользователи о ней знают. Если отключить эту опцию, то камера не будет запрашивать авторизацию при подключении к ней, что сделает ее уязвимой для взлома. Стоит отметить, что встречаются камеры с двойной авторизацией для http-доступа и для доступа по протоколу ONVIF. Также в некоторых камерах существует отдельная настройка для запроса авторизации при подключении по прямой RTSP-ссылке.
5. Защита сети. Необходимо правильно настраивать коммутирующее оборудование. Сейчас большинство коммутаторов поддерживают защиту от arp spoofing — обязательно используйте это.
6. Включение OSD-меню. Необходимо включать OSD-меню с текущим временем и датой на камере, чтобы всегда можно было проверить актуальность изображения. Это хороший способ защиты именно от замены видеоряда, так как OSD накладывается на все видео, идущее с определенной камеры. Даже когда злоумышленник запишет RTSP-поток, подмена будет заметна благодаря данным, которые все равно останутся на видеокадрах.

8.2. ОХРАНА И СИГНАЛИЗАЦИЯ

Безопасность – это состояние системы или объекта, при котором воздействие внешних и внутренних факторов не нарушает его деятельности. В настоящее время существует множество объектов частной и государственной собственности, которые используют охранные системы безопасности разного типа. Для осуществления охраны разработаны различные системы, которые можно разделить на отдельные виды:

- системы оповещения;
- системы охраны для дачи;
- охранные системы для частных домов;
- системы пожаротушения;
- источники питания системы охранно-пожарной сигнализации;
- GSM-системы охраны объектов;
- системы видеонаблюдения.



8.2.1. Охранные системы безопасности

Охранные системы безопасности могут быть нескольких видов:

- автономная сигнализация;
- системы охранной сигнализации с использованием GSM;
- охранная сигнализация с передачей сигнала по телефонной линии.

Автономная сигнализация состоит из датчиков фиксирующих нарушение режима охраны. При срабатывании системы генерирует световые и звуковые сигналы, предупреждая соседей о незаконном проникновении на жилой объект. В данном случае соседи должны вызвать охрану или полицейский наряд для проверки объекта, где сработала сигнализация. Охранные системы для частных домов позволяют повысить защищенность имущества и снизить случаи краж.

Система охранной сигнализации с использованием GSM сигнала. При установке данной системы охраны используется мобильная связь. Сигнал тревоги поступает владельцу объекта и на пульт охраны организации осуществляющей безопасный режим

эксплуатации и защиту домовладения. Система охранной сигнализации с использованием телефонной линии, действует по тому же принципу. Сигнал о нарушении режима передается на пульт охраны, которая выезжает на объект и осуществляет его проверку.

Охранная система для передачи сигнала использует специальный защищенный канал с частотой 433 МГц, который поступает с датчиков фиксации вторжения на объект.

В доме могут быть установлены различные датчики:

- инфракрасный пассивный датчик движения, фиксирует перемещение теплового излучения по помещению;
- датчики контактные магнитные;
- датчики реагирования на дым;
- датчики реагирования на перемещение объекта с передачей сигнала на радиочастоте;
- датчики вибрационные реагирующие на малейшие колебания;
- датчики лучевые инфракрасные реагируют на пересечение лазерного луча посторонним объектом.

Необходимо отметить, что датчики, используемые в проводной системе, имеют больший радиус обнаружения и фиксации нарушений режима охраны. Для проводных датчиков установлена предельная дальность срабатывания не более 100 метров.

8.2.2. Использование систем видеонаблюдения

Для постоянного контроля объектов используются системы видеонаблюдения с видеокамерами. Видеонаблюдение можно производить в режиме on-line, а также фиксировать все события на видеорегистратор.

В состав комплекта для видеонаблюдения входят:

- камеры (аналоговые или цифровые) в количестве от 2 до 8 шт.;
- видеорегистратор;
- блок питания;
- соединительные провода;
- блок контроля и управления.

Камеры могут устанавливаться внутри дома и по периметру участка.

8.2.3. GSM-системы для охранной сигнализации

Для передачи сигнала GSM-системы охраны используют сеть GSM/Wi-Fi, которая способна работать при температуре от -40*С до +50*С и отличается высокой надежностью. GSM-система может комплектоваться IP-камерой, которая работает в сети Wi-Fi и использует GSM связь, как дополнительный канал передачи сигнала.

Использование охранных систем безопасности значительно повышает уровень защищенности домов и обеспечивает сохранность имущества.

8.3. УЯЗВИМОСТИ ОХРАНЫ И СИГНАЛИЗАЦИЙ

СИГНАЛИЗАЦИЯ

95% сигнализаций присутствующих сегодня на рынке взламываются устройством под названием «мануфактурный кодграббер»

Время взлома: до 5 сек.

БЛОКИРАТОРЫ

Механические блокираторы установленные на АКПП, рулевом валу и капоте удаляются методом "бампинга" и с помощью отмычек.

Время взлома: до 40 сек.

ИММОБИЛАЙЗЕР

Автоугонщики обходят штатный доп. иммобилайзер методом подмены блока управления двигателя в салоне автомобиля.

Время взлома: до 55 сек.

GPS ОХРАНА

Любая спутниковая охранная система бесполезна, если злоумышленники используют Подавитель сигнала GPS (антитрекер GPS)

Время взлома: до 3 сек.

СЕКРЕТКА

Секретка (кнопки - прерыватель цепи) обходится методом проброса провода из колодки управления к заблокированному устройству.

Время взлома: до 90 сек.

GSM ОХРАНА

Любая сотовая (GSM) охранная система бесполезна, если злоумышленники используют Подавитель GSM (900/1800), TDMA, CDMA, UMTS

Время взлома: до 3 сек.

8.3.1. Защита от перехвата GSM-сигнала

Существует три поколения беспроводной связи: 2G, 3G, 4G. Самый популярный стандарт – это 2G, то есть у него самая большая зона покрытия. Он был введён в эксплуатацию в начале девяностых. Так как этому стандарту более двадцати лет, то у него существует ряд проблем с безопасностью: односторонняя аутентификация и возможность установки соединения без шифрования.

Есть телефон и базовая станция. У телефона на сим-карте записан неизвлекаемый ключ, с помощью которого происходит аутентификация. Со стороны оператора для каждой аутентификации генерируется случайное число, sres и сессионный ключ шифрования (Kc). Базовая станция передаёт случайное число телефону, телефон передаёт сим-карте. Сим-карта, в ответ, возвращает два значения – sres и Kc. Sres возвращается оператору. Сравнивая sres, оператор идентифицирует абонента. После этого выдаётся команда на шифрование, которое происходит с помощью Kc.

Из вышеизложенного алгоритма видно: ничто не мешает подменить базовую станцию, заменить шифрование отсутствием шифрования. Используя данную уязвимость, злоумышленник может нас слушать. Для осуществления полноценного перехвата понадобится виртуальная базовая станция (BTS), дешифратор и эмулятор телефона. Перехватчик в виде такой системы обойдётся достаточно дорого.

Может быть использован упрощённый вариант. Есть виртуальная базовая станция и интернет. Через интернет по VoIP осуществляется перехват. Данный вариант имеет ряд ограничений. То есть связь будет односторонняя. Через VoIP абонент сможет звонить, но не сможет принимать вызовы.

При помощи этой уязвимости ещё можно осуществлять IMSI-Catcher и блокиратор сигнала. IMSI-Catcher – это система, которая получает идентификаторы мобильных устройств в радиусе действия и даёт им отбой. То есть абоненты возвращаются в сеть реального оператора связи, но идентификаторы их получены. Блокиратор сигнала работает примерно также как и IMSI-Catcher, но после процесса аутентификации принимает абонента. Абонент находится на данной виртуальной базовой станции и ему не доступны никакие сервисы.

Существует ряд признаков перехвата сигнала:

1. Мощный сигнал.
2. Большой коэффициент C2. Коэффициент C2 используется оператором для балансировки нагрузки между сотами.
3. Отсутствие Paging Request. Это пакеты, отвечающие за запрос установления канала с абонентом.
4. Отсутствие сервисов (EDGE, USSD и так далее).
5. Определение «глушилки» (подавитель сигнала).
6. Отсутствие соседей (все соседи из другого LAC).
7. Отсутствие шифрования.
8. Открытие канала без совершения транзакции.

Учитывая все эти признаки, можно попытаться найти злоумышленника при помощи SDR. Это радио-платформа, которая позволяет настраиваться на нужную частоту, принимать сигнал, демодулировать и декодировать его уже на компьютере. На выходе мы можем получать спектр и широковещательный канал. По стандарту GSM есть ряд радио-сигналов, которые должны соблюдаться для электромагнитной совместимости. Соответственно, просмотрев спектр, выявляются признаки перехвата. Анализируя их, можем сделать вывод: находимся мы на реальной базовой станции или на виртуальной.

8.3.2. "Перехват меток"

Электронно-магнитная метка опрашивается датчиком в транспортном средстве с расстояния в несколько десятков сантиметров. Метка-транспордер (RFID) считывается злоумышленниками направленной антенной, проволочным контуром со считывающим устройством, который находится у "случайного прохожего". Злоумышленник пройдет в магазине рядом, нажав при приближении кнопку активации считывания - Вы даже не заметите! А намагничивание и программирование новой метки - секундное дело.

Даже метки-транспордеры с уникальной динамической диалоговой идентификацией типа "свой-чужой" подвергаются электронному взлому. Видимо, и эти современные алгоритмы становятся собственностью злоумышленников.

8.3.3. Взлом современных GPS сигнализаций

Все GPS и ГЛОНАСС системы используют для работы триангуляционную систему, для корректной работы системы необходимо от 3 спутников, которые отслеживают нахождение объекта на поверхности земли.

Система триангуляции обладает максимальной точностью: положение неподвижного или движущегося объекта определяются с погрешностью до нескольких сантиметров. Немаловажно, что системы слежения делятся два вида спутниковых систем: военная (предназначенная для военных операций и боевых действий) и гражданская системы.

Частоты GPS и ГЛОНАСС являются элементарными радиосигналами на частоте 1575.42 МГц, они могут быть заблокированы посредством специального технического устройства - глушилки GPS и ГЛОНАСС сигналов. Сегодня любой житель крупного мегаполиса и небольшого населенного пункта может купить подавитель-глушилку GPS-сигнала через интернет с доставкой курьером на дом. Стоимость такого девайса не превышает 40$. В просторах интернета полно подробных инструкций и схем изготовления таких устройств. Любой автовор обладающий поверхностными знаниями в радиоэлектронике сможет собрать глушилку в домашних условиях.

При использовании глушилок и подавителей ваша GPS сигнализация и автономные GPS-трекеры, отслеживающие местоположение авто становится бесполезной игрушкой - из-за создаваемых помех в эфире определение координат нахождения транспортного средства охранной системой становится невозможным. Если злоумышленники не используют совместно с GPS-глушилок GSM-подавитель, то данные охранные системы будут отсылать ложные (неправильно определенные координаты) вам или на пульт охраны это даст преимущество злоумышленникам, и достаточно времени для того чтобы досконально разобрать всю машину и деактивировать все охранные системы без особой спешки.

8.3.4. Обход охранных извещателей

Любая автоматическая охранная система состоит из датчиков, которые регистрируют нарушения, и устройства, которое получает сигнал от них. За время своего существования охранные извещатели (или датчики, как их чаще называют в народе) совершенствовались, и теперь обойти их не так просто.

Самый распространённый тип охранных систем – это так называемые датчики движения, которые в научной литературе называются инфракрасными извещателями. Принцип их действия заключается в следующем: инфракрасный луч прочёсывает пространство в поисках теплового излучения, и если оно зафиксировано, то извещатель

сообщает о том, что в охраняемом периметре появился нарушитель. Если человек пересекает местность, то его излучение мгновенно регистрируется датчиком, а значит, пройти мимо подобного устройства очень непросто.

Чаще всего инфракрасные датчики вешают на потолок или на стену. Для того чтобы закрепить извещатели, используются кронштейны. Выделяют активные и пассивные извещатели. Активные датчики чаще всего используются для охраны больших периметров (до 100 метров), а пассивные – это самый распространенный вид охранных систем.

Один из самых старых и проверенных способов обхода датчиков – это экранирование. Для того чтобы датчик не засёк вашего излучения, следует закрыться от него. В этом случае вам поможет обычная простыня или кусок стекла. Правда, нужно, чтобы ни одна часть тела не высовывалась за пределы экрана. Например, к стеклянной поверхности крепятся присоски, за которые его и нужно держать. Такой вариант срабатывает только тогда, когда нарушитель знает, в каком месте расположены датчики движения. Если датчик помещён на потолке, то закрывать себя следует сверху, а если на стене – то сбоку.

Экранировать можно и сам извещатель. Например, аккуратно закрыв его книгой или залив краской из баллончика. Правда, предварительно вам придётся подобраться как можно ближе к датчику и при этом остаться незамеченным. Чаще всего для экранов выбирают акрил, чёрную бумагу, винил или другие материалы. В принципе, скрыть тепловой луч от датчика может практически любая поверхность, которая будет размещена между ним и нарушителем.

Второй способ остаться незамеченным для датчика движения – это двигаться с перерывами. В инструкции к инфракрасному извещателю можно увидеть такую строку: датчик фиксирует цель, которая движется со скоростью от 0,1 до 5 метров в секунду (некоторые версии датчиков имеют даже меньший диапазон). Если двигаться рывками, то есть перемещаться за секунду на один или полметра, а затем пару секунд оставаться на месте, то датчик движения не увидит вас.

Если инфракрасный датчик установлен на заборе или другом ограждении, то его можно обойти двумя способами. Первый – это прорезать отверстие в ограждении. Обычно датчик фиксирует только попытки перелезть через забор, а вот деформация самого ограждения его не интересует. Второй способ заключается в приставной лестнице, которая должна быть выше забора на метр или хотя бы 80 см. Датчики, которые устанавливаются на ограждении, фиксируют только близкое тепловое излучение, так что если перелазить через забор выше, то извещатели этого не заметят. Такой метод отлично срабатывает для не очень высоких ограждений, для которых достаточно подставить невысокую раскладную лестницу.

8.4. ЗАЩИТА ОТ ТЕХНИЧЕСКИХ СРЕДСТВ НЕГЛАСНОГО СЪЕМА ИНФОРМАЦИИ

Защита от технических средств негласного съема информации (НСИ) – комплекс мероприятий, направленный на создание условий, предотвращающих перехват защищаемой информации техническими средствами разведки.

По принципу действия все технические средства пространственного и линейного зашумления можно разделить на 3 большие группы:

- средства создания акустических маскирующих помех;
- средства создания электромагнитных маскирующих помех;
- средства противодействия лазерным системам НСИ.

8.4.1. Генераторы шума в акустическом диапазоне

Принцип действия указанного генератора основан на создании с помощью специального генератора маскирующей помехи в речевом диапазоне, перекрывающей спектр человеческой речи (50 – 7 000 Гц) “Белый Шум”.

Преимущества:

- простота;
- практическая невозможность избавления от помехи.

Воздействие на записывающие устройства:

- силовое;
- маскирующее (информационный сигнал совмещен с шумом).

Недостатки:

- невозможность комфортного проведения переговоров;
- малое время работы с устройством (10-15 мин);
- человеческий фактор: попытка перекричать устройство защиты снижает эффективность его применения.

Эти устройства используются крайне редко, когда нет времени проверять помещение на наличие записывающих устройств.

Так же используются как дополнительные средства защиты:

- дверных проемов;
- межрамного пространства окон;
- систем вентиляции.

8.4.2. Устройства виброакустической защиты

Наиболее эффективным средством защиты помещений, предназначенных для проведения конфиденциальных мероприятий, от съема информации через оконные стекла, стены, системы вентиляции, трубы отопления, двери и т.д. являются устройства виброакустической защиты. Они позволяют предотвратить возможное прослушивание с помощью проводных микрофонов, звукозаписывающей аппаратуры, радиомикрофонов и электронных стетоскопов, лазерного съема акустической информации с окон.

Противодействие прослушиванию обеспечивается путем внесения виброакустических шумовых колебаний в элементы конструкций зданий.

Принцип работы:

Генератор формирует белый шум в диапазоне звуковых частот. Передача акустических колебаний на ограждающие конструкции производится при помощи пьезоэлектричеких или электромагнитных вибраторов с элементами крепления. Конструкция и частотных диапазон излучателей должны обеспечивать эффективную передачу вибрации.

8.4.3. Устройства ультразвукового зашумления

Отличительной особенностью этих средств является воздействие на микрофонное устройство и его усилитель достаточно мощным ультразвуковым сигналом (группой сигналов), вызывающим блокирование усилителя или возникновение значительных линейных искажений, приводящих в конечном счете к нарушению работоспособности микрофонного устройства (к его подавлению).

8.4.4. Средства создания электромагнитных маскирующих помех

Применяются для перекрытия канала утечки через побочное электромагнитное излучение и наводки персональных ЭВМ и периферийных устройств, а так же другой оргтехники посредством создания помех в широкой полосе частот.

Недостатки:

Создание непреднамеренных помех широкому классу радиоэлектронных устройств, расположенных в непосредственной близости от передатчика маскирующих излучений

Различают:

- линейного зашумления;
- пространственного зашумления.

1. локальные;
2. глобальные.

8.4.5. Средства противодействия лазерным системам НСИ

Пассивные:

1. Использование естественных препятствий;
2. Использование погодных условий;
3. Разнесение;
4. Использование просветленной пленки;
5. Использование зеркальных пленок.

Активные:

Заключаются в введении в оконные стекла шумовых виброколебаний.