МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему «Защита объектно-ориентированных систем хранения данных»

Исполнитель Везолайнен Александр Олегович
(фамилия, имя, отчество)

Руководитель к.т.н., доцент
(ученая степень, ученое звание)

Шапаренко Юрий Михайлович
(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____
(подпись)

д.т.н., профессор
(ученая степень, ученое звание)

Бурлов В.Г.
(фамилия, имя, отчество)

«17» февраля 2017 г.

Санкт–Петербург

2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему «Защита объектно-ориентированных систем хранения данных»

Исполнитель Везолайнен Александр Олегович
(фамилия, имя, отчество)

Руководитель к.т.н., доцент
(ученая степень, ученое звание)

Шапаренко Юрий Михайлович
(фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____

(подпись)

д.т.н., профессор
(ученая степень, ученое звание)

Бурлов В.Г.
(фамилия, имя, отчество)

«___»_____20__г.

Санкт–Петербург

2017

Оглавление

ВВЕДЕНИЕ

Актуальность темы данной дипломной работы определяется возросшим уровнем проблем и задач инф. безопасности даже в условиях быстрого роста науки и технологий и инструментальной базы для защиты персональных данных.

Неосуществимо обеспечить абсолютно стопроцентный уровень защиты корпоративных информационных систем, при этом предупредительно расставив приоритеты в задачах по защите информации в обстоятельствах ограниченности доли бюджета, которая выделяется на информационные технологии.

Надежная защита вычислительной и общесетевой корпоративной инфраструк туры считается базисной проблемой в сфере информативной защищенности с целью каждый фирмы. С увеличением коммерциала компании и перехода к регионально-
расчисленной организации она начинает выступать за рамки отдельного соор ужения.

Результативная защита IT-инфраструктуры
и практических корпоративных систем на сегодняшний день
неосуществима без внедрения современный технологий контроля сетевого до ступа. Участившиеся случаи кражи носителей, включающих значимые и конфиденциальные сведения делового характера, все без
исключения более вынуждают осуществлять организационные мероприятия.

Целью данной работы будет оценить смарт-станцию Tellus и разработать мероприятия по её защите от каких-либо угроз извне.

Поставленная цель обуславливает следующие задачи дипломной работы:

1)рассмотреть объект (смарт-станцию Tellus);

2)проанализировать смарт-станцию Tellus на уязвимости к каким-либо воздействиям;

3)рассмотреть виды возможных угроз

4)выявить способы защиты смарт-станции и дать рекомендации

Глава 1 Общие понятия о смарт-станции, её настройка и подключение.

1.1 Общие понятия.

Смарт-станция Tellus – многофункциональное устройство с функциями мини IP АТС для организации телефонии и Internet-доступа на предприятии, фирме или дома.

С помощью смарт-станции вы сумеете:

-Сформировать офисную МИНИ-АТС на базе аналоговой и/или IP-телефонии;

-Подсоединить вплоть до пяти абонентов DECT-трубок;

-Сформировать беспроводную сеть Wi-Fi с
целью допуска к Интернету, функционирующую в 2-х диапазонах частот 2.4-2.5Ггц и 5Ггц;

-Сформировать локальную сеть с перспективой гостевого допуска;

-Прибегнуть к сервису приёма факсов в e-mail;

-Подсоединить печатающее устройство,
сканер и прочие приборы и обеспечить к ним единый доступ;

-Материализовать сетевое хранилище сведений NAS и единый доступ к USB-накопителю

1.2 Перечень возможностей смартстанции TELLUS

Ниже приведены функции и возможности рассматриваемой смартстанции:

Автоматизированный подбор маршрута звонка – Функция IP-телефонии, дозволяющая при звонке автоматом искать более практичный тариф и оператора связи, к примеру, при подборе среди муниципальной телефонной сети, междугородней связи и звонками за границу. Для любой группы звонков может быть установлено условие совершения звонка – в данном случае Tellus сам установит, по какой линии следует осуществить звонок.

Блокировка нежелательных вызовов – Возможность создания «черного списка» контактов, в который входят звонки, нежелательные для получения.

Гостевой Wi-Fi доступ - создание отдельной бес проводной сети доступа к Internet для гостей. Главным образом применяется для обеспечения информационной безопасности внутри корп. и/или домашней сети, а также для резерва ширины канала передачи данных пользователей сети, которые подключаются постоянно.

Голосовое меню и шлюзование (DISA) - Возможность интерактивного ведения диалога во время приёма поступающих звонков посредством использования кнопок телефонного аппарата в тональном режиме.Это даёт возможность настроить автоматическую переадресацию на внутренние номера автоматической телефонной станции при общем внешнем номере телефонной линии.

Двухчастотный диапазон WLAN 2.4Ггц и 5Ггц - Возможность установки двух частотных режимов бес проводной сети - 2.4 Ггц и 5 Ггц, которые влияют на скорость передачи каких-либо данных внутри сети. 5 ГГц позволяет повысить скорость передачи данных на некоторую величину.

Перевод вызовов - Возможность переключения звонка от одного абонента на других внутри сети.

Протокол IP (Internet Protocol) – Протокол, с помощью которого осуществляется передача данных по сети.

Система распределения входящих вызовов – даёт возможность рассредоточить входящие телефонные вызовы среди абонентов внутри сети Tellus (DECT, IP-телефония, мобильны телефоны).

Смартстанция (Smartstation) – это тип электронных многофункциональных устройств, одновременно заменяющее Wi-Fi роутер, ADSL модем (как вариант), VoIP шлюз, мини АвтоТелеСтанцию, DECT базу и с поддержкой использования сетевого хранилища и сетей 3G/4G. Интерфейс смартстанции даёт возможность настроить устройство под индивидуальные и личные предпочтения пользователя.

Факс-машина - Возможность получения факс-сообщений в цифровом виде (pdf,jpg) на e-mail.

CNG (Comfort Noise Generation) - Технология генерации комфортного шума при разговоре по телефону.

DECT (Digital Enhanced Cordless Telecommunication) - Технология беспроводной телефонной связи для радиотелефонов, встроенная в Tellus

DECT-станция даёт возможность подключить до 6 телефонных трубок.

Переадресация вызовов - Возможность автоматической переадресации звонка с телефонного отдельного номера на номера других абонентов (включая, мобильны телефоны).

DHCP (Dynamic Host Configuration Protocol) - сетевой протокол, дающий возможность компьютерам автоматически получать IP-адрес и другие параметры и опции, необходимые для работы в сети. С точки зрения пользователя, данный протокол позволяет настроить локальную домашнюю сеть совершенно автоматически без необходимости какого-либо ручного ввода настроек для каждого подсоединённого устройства.

DMZ (Demilitarized zone) - Технология обеспечения защиты информационной безопасности. При этом запросы из сети Internet переадресуются на установленные пользователем устройства локально сети.

DTMF (Dual-Tone Multi-Frequency) - Функция тонального набора в телефоне для управления голос. меню и использования ip-телефонии.

Dyn DNS (Dynamic Network Services) - Сервис, который позволяет пользователям получить доступ из внешней сети к компьютеру, который не имеет постоянный IP-адрес.

DECT база – возможность подсоединения к Tellus беспроводных трубок DECT (до 6 шт.), в этом случае Tellus выступает в роли телефонной станции для внутренних абонентов с внеш. линией для входящих и исходящих звонков.

Ethernet - Технология физического соединения компьютеров и устройств для объединения в локальную сеть и/или для доступа к сети Internet. Каждый из 5

портов Ethernet на задней панели Tellus поддерживает скорость передачи данных около 1 Гбит/с.

Firewall – система информационной безопасности, которая позволяет открывать/закрывать порты, а также ограничивать доступ к некоторым или опред. ресурсам, ограничивать сетевую активность каких-либо приложений, ограничивать скорость соединения и вести учет трафика.

FTP (File Transfer Protocol) – технология доступа к информации на удаленный ПК и/или сервере, дозволяющая сформировать сервер с целью хранения и обмена данными между участниками сети. Понадобится подключение наружного USB устройства для хранения данных.

FXO (Foreign Exchange Office) и FXS (Foreign Exchange Station) – разъёмы для подключения к Tellus телефонной линии, позволяющей в одно и то же время использовать телефон и факс (модем, МФУ). В случае, если Tellus будет выключен, то телефонная линия будет продолжать работать.

LAN (Local Area Network) - Локальная вычислительная сеть для соединения компьютеров и сетевых устройств друг с другом.
На задней панели смартстанции размещены 4 порта LAN, что позволяют пользоваться им, как полноценным коммутатором или маршрутизатором устройств.

L2TP (Layer 2 Tunneling Protocol) – является одним из средств создания VPN-соединения, аналогичное PPTP, однако предоставляет более защищенное соединение для пользователей, нежели PPTP.

MU-MIMO (Multi-user MIMO) – Технология параллельной передачи пакетных данных в одно и то же время сразу нескольким пользователям бес проводной сети с более высокой скоростью.

MultiSSID (Multi Service set identification) - Возможность формирования нескольких беспроводных сетей, в том числе для гостей с разграничением прав доступа к некоторым сетевым ресурсам.

NAS (Network Attached Storage) - Возможность подключения внешнего хранилища данных к смартстанции. Это позволит всем необходимым устройствам, подключенным к ней, иметь бесперебойный доступ к хранилищу данных как по локальной сети, так и удаленно.

NAT (Network Address Translation) - механизм, подменяющий сетевой адрес компа или устройства в локальной сети, присваивая ему уникальный адрес в глобальной сети, обходя барьеры (роутер, модем, маршрутизатор и т.д.).

PAT (Port Address Translation) - Технология статической трансляции портов, которая позволяет получить доступ к локальной сети из сети Internet.

Port Forwarding - Технология, схожая с DMZ, при которой запросы пересылаются только на те конкретные порты, которые были выбраны пользователем.

PPPoE (Point-to-point protocol over Ethernet) - аналог модемного dial up-соединения с передачей данных по Ethernet со скоростью до 100 мбит/с. Так как принципом работы PPPoE является установление виртуального соединения поверх физического соединения Ethernet, то процесс работы PPPoE разделяется на две стадии:
В 1й стадии два устройства сообщают друг другу свои сетевые адреса и устанавливают начальное соединение.
Во 2й стадии уже запускается обмен данными между устройствами.

PPTP (Point-to-Point Tunneling Protocol) - одно из средств создания VPN-соединения. Даёт возможность создавать защищенные каналы для обмена данными по различным сетевым протоколам между устройствами. В обыденном использовании наиболее часто встречается для доступа в сеть Internet и удаленного доступа внутри локал. сети.

SIP (Session Initiation Protocol) - Телефонная книга, в которой абсолютно каждому абоненту дан свой уникальный адрес, по которому можно звонить и принимать звонки посредством софтфона или мобильного приложения для IP-телефонии.

SMB (Server Message Block) - Протокол для удаленного доступа к периферийным устройствам и компьютерам, подключенным друг к другу по сети.

UPnP (Universal Plug and Play) – технология автоматического распознавания каких-либо подключаемых устройств.

USB (Universal Serial Bus) - Разъём для подсоединения сетевых устройств и передачи данных между ними внутри локальной сети. На задней панели смартстанции расположены 2 порта USB и это позволяет в одно и то же время подключать несколько устройств (например, принтер+флеш-память).

VAD (Voice Activity Detection) - Технология обнаружения "молчания" при передаче голоса по каналам радиосвязи или в пакетных сетях, что делает общение по телефону более комфортным так как исключаются потери данных.

VLAN (Virtual Local Area Network) – виртуальная локальная компьютерная сеть, которая создаётся для обеспечения безопасности и удобства администрирования аккаунтов пользователей.

VPN (Virtual Protected Network) - создание виртуальных защищённых сетей, для защиты данных при их передаче в незащищенной среде, к примеру в сети Internet. Цель VPN – обеспечить прозрачный доступ к ресурсам сети, где пользователь сможет безопасно совершать в сети привычные ему действия вне зависимости от того, насколько он далеко находится. Это и есть причина из-за которой VPN весьма популярен среди дистанционных работников и офисов, которым необходимо совместное использование ресурсов территориально разделённых сетей.

WAN (Wide Area Network) – это разъём для высокоскоростного подключения к сети Internet (вплоть до 1 Гбит/с) по технологии Ethernet или ADSL.

WLAN (Wireless Local Area Network) - Беспроводная локальная сеть Wi-Fi или WiMAX, которая позволяет объединять устройства и получить доступ к сети Internet.

WLAN 802.11 a/b/g/n - Возможность подключения к Wi-Fi сети устройств, что поддерживают какой-либо из указанных стандартов (a/b/g/n). Нынешние устройства поддерживают технологию 802.11g или 802.11n. Они отличаются скоростью передачи данных внутри сети от 54 мбит/с до 300 мбит/с.

WLAN Broadforming - Технология увеличения скорости передачи данных беспроводной сети для отдельного устройства (компьютера) за счет изменения направления антенн беспроводной связи. Таким образом, зона покрытия Wi-Fi оптимально подстраивается под текущее расположение пользователей.

1.3 Первичная настройка станции и подключение.

1. Необходимо закрепить смартстанцию на подставке и подключить её к питанию, а затем подключить к компьютеру (ноуту, планшету…).

2. Соединить разъём Ethernet сетевой карты ПК и один из четырёх разъёмов LAN на задней панели смартстанции спец кабелем из комплекта поставки.

3. Для подключения к смартстанции по сети Wi-Fi необходимо открыть на компьютере (ноутбуке, планшете…) список доступных беспроводных сетей, затем выбрать сеть «Tellus Wi-Fi» (для диапазона 2.4-2.5 ГГц) или «Tellus Wi-Fi 5» (для диапазона 5ГГц) и подключиться к выбранной сети, используя пароль или функцию WPS, если подключаемое устройство поддерживает её.

4. Подключить Tellus к сети Internet. Подключить кабель Интернет провайдера к разъёму WAN Tellus.

5. Подключить городскую телефонную линию (при её наличии) к Tellus. Подключить телефонную линию к разъёму Line. Телефон подключить к разъёму Tel1 или Tel2.Связь по телефонной аналоговой лини доступна доступна даже при отключённом питании Tellus.

6. Подключить принтер (сканер или другие USB-устройства). Подключить ихк к одному из двух разъёмов USB 2.0.

7. Войти в Web-интерфейс управления Tellus. Для входа в Web-интерфейс управления Tellus необходимо ввести в адресной строке любого Internet-браузера доменное имя устройства «Tellus» (задано по умолчанию, можно поменять впоследствии) – http://tellus/ или IP-адрес http://192.168.10.1/ и нажать Enter.

8. Задать пароль для доступа к Web-интерфейсу управления Tellus в поле «пароль» и повторить его в поле «повторить пароль». Пароль должен состоять не менее чем из трёх символов. Рекомендуется использовать

сложный пароль, состоящий из букв разного регистра и цифр. После нажатия кнопки «Войти» вы попадёте на стартовую страницу Web-интерфейса управления смартстанции Tellus.

Теперь смартстанция готова к работе. Более подробная настройка функций и возможностей представлена в руководстве пользователя.

Глава 2. Выявление уязвимостей смарт-станции

2.1 Анализ угроз защищённой передачи данных в беспроводных сетях.

Проблема обеспечения безопасности – является одной из основных при построении беспроводных сетей. Этому способствуют 2 фактора.

1)Повсеместное распространение сети Internet. К этой сети подключено огромное количество компьютеров. В будущем их количество увеличится во много раз, по этой причине вероятность доступа хакеров к уязвимым компьютерам и компьютерным сетям также постоянно увеличивается. Помимо этого, широкое распространение Internet даёт возможность хакерам обмениваться информацией в глобальном масштабе.

2)Всеобщее распространение лёгких в использовании ОС и сред разработки. Этот фактор резко понижает требования к уровню знаний злоумышленника. Раньше хакеру были необходимы хорошие знания и навыки программирования, для создания и распространения вредоносных программ. Теперь же, для получения доступа к хакерскому средству, нужно просто знать IP-адрес нужного сайта, а для проведения атаки достаточно щелкнуть мышкой.

Если в обычных сетях данные передаются по кабелям, то радиоволны, которые используются в беспроводных сетях, достаточно легко перехватить, если иметь соответствующее оборудование. При использовании беспроводного доступа к локальной сети угрозы безопасности сильно возрастают. Схема возможных атак на беспроводную сеть WLAN приведена на рисунке 2.1

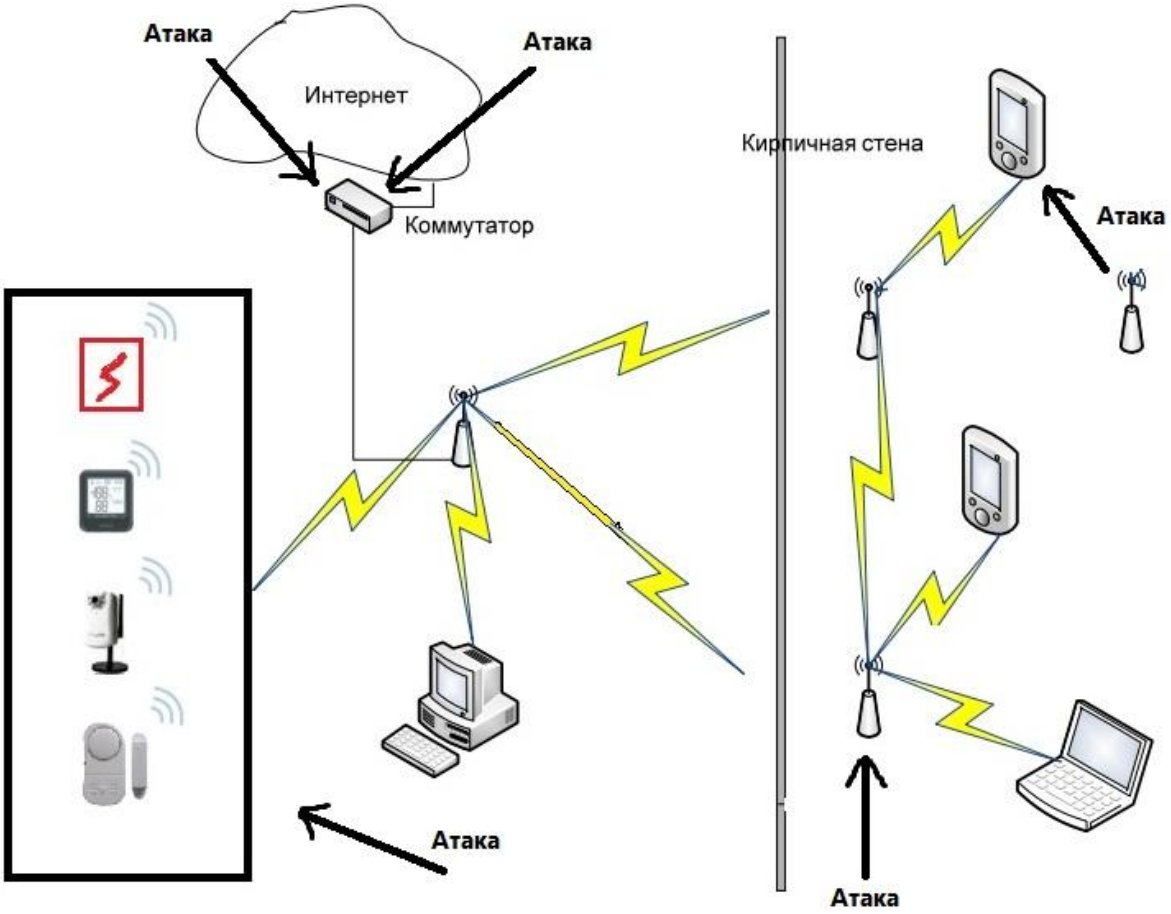

Рисунок 2.1 – моделирование атак на беспроводную сеть WLAN

Необходимо отметить основные уязвимости и угрозы для беспроводных сетей.

– Вещание радиомаяка**.** Точка доступа включает с определенной частотой широковещательный радиомаяк, для оповещения окрестных беспроводных узлов о своем присутствии. Эти широковещательные сигналы включают в себя основную информацию о точке беспроводного доступа,и это как правило, SSID, и приглашают беспроводные узлы зарегистрироваться в текущей области. Абсолютно любая рабочая станция, которая находится в режиме ожидания, имеет возможность получить SSID и добавить себя в соответствующую сеть.

Вещание радиомаяка является «врожденной патологией» беспроводных сетей. Многие модели дозволяют отключать содержащую SSID часть этого вещания, чтобы немного затруднить беспроводное подслушивание, но SSID, как бы то ни было, посылается при подключении, именно по этой причине все равно существует небольшое окно уязвимости.

– Обнаружение WLAN. Для обнаружения беспроводных сетей WLAN используется, к примеру, утилита NetStumber вместе со спутниковым навигатором глобальной системы позиционирования GPS. Данная утилита идентифицирует SSID сети WLAN, а также может установить, используется ли в ней система шифрования WEP. Применение внешней антенны на ноутбуке даёт возможность обнаружения сетей WLAN во время обхода нужного района или поездки по городу. Надежным методом обнаружения беспроводных сетей является обследование здания офиса с ноутбуком в руках.
– Ложные точки доступа в сеть**.** Опытный хакер может создать ложную точку доступа с имитацией сетевых ресурсов. Абоненты, ничего не зная, будут обращаться к этой ложной точке доступа и сообщать ей свои важные реквизиты, например аутентификационную информацию. Этот тип атак могут применять в сочетании с прямым «глушением» настоящей точки доступа в сеть.
– Отказ в обслуживании**.** Полный паралич сети может вызвать атака типа DoS (Denial of Service) — отказ в обслуживании. Цель такой атаки состоит в создании помехи при доступе пользователя к каким-либо сетевым ресурсам. Беспроводные системы особенно восприимчивы к атакам такого типа. Физический уровень в беспроводной сети — абстрактное пространство рядом с точкой доступа. Злоумышленник может включить устройство, которое заполнит весь спектр на рабочей частоте помехами и нелегальным трафиком — это не вызывает особых

трудностей. Кроме того факт проведения DoS-атаки на физическом уровне в беспроводной сети очень сложно доказать.

– Анонимный доступ в Интернет**.** Незащищенные беспроводные сети дают хакерам идеальный анонимный доступ для атак через сеть Internet. Хакеры имеют возможность использовать незащищенную беспроводную сеть организации для выхода через нее в Internet, где они будут совершать противозаконные действия, не оставляя при этом никаких следов. Организация с незащищенной сетью фактически становится источником атакующего трафика, который нацелен на другую компьютерную систему, и это связано с потенциальным риском правовой ответственности за нанесённый ущерб жертве атаки хакеров.

2.2.2 Анализ угроз защищённой передачи данных в проводной телефонной линии.

Наиболее распространённый вид промышленного шпионажа – контроль и прослушка телефонных разговоров. Малые финансовые затраты , а также малый риск реализации угроз, разнообразные способы и места для съёма информации и необязательность захода в контролируемое помещение и проч.

Контролировать телефонные разговоры является возможным на всей протяжённости телефонной линии.

Средства перехвата, которые предлагают на российском рынке, реализуют различные физические принципы и современные программно-аппаратные решения, коими являются: разные устройства контактного и бесконтактного присоединения к телефонным линиям; специальные телефонные "жучки" и ответчики; комплексы перехвата сотовой связи во всех стандартах.

Объекты телефонной сети (АТС, телефонные аппараты) могут подвергаться следующим атакам и методам съёма информации:

– Физическое нарушение телефонной линии

Такой вид угрозы очень опасен и приводит к краху всей проводной телефонной линии. Организуется такая атака простым обрывом телефонного кабеля, тем самым управляющие сигналы по телефонной линии передаваться прекращаются.

– Способ непосредственного подключения

Является самым простым и распространённым способом телефонных разговоров. Шунт подслушивающего устройства может быть установлен в любом месте, откуда имеется доступ к телеф. проводам или телефону: в телефонной розетке или в любом другом месте телефонной линии на всей её длине до распределительной коробки. В техническом плане самым простым способом незаконного подключения можно назвать контактное подключение, представленное на рисунке 2.2 [14].

– Подключение бесконтактным методом

Для того, чтобы устранить недостаток, связанный с влиянием подключенного устройства на характеристики линии связи, обычно используется бесконтактный метод, а для съема информации обычно применяется индуктивный датчик, который выполнен в виде трансформатора. Схема такого подключения показана на рисунке 2.3 [14].

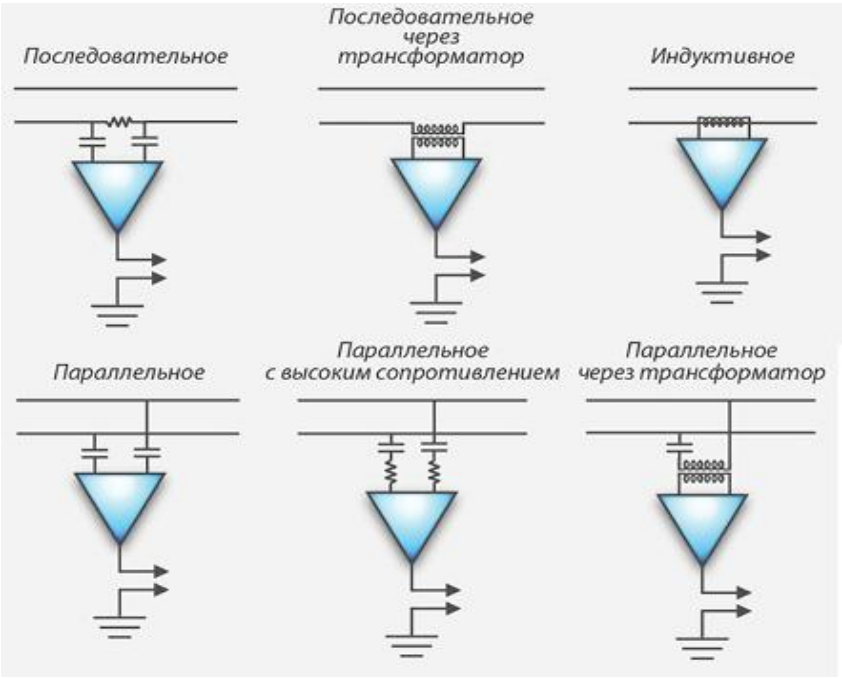

Рисунок 2.2 – Варианты контактных подключений устройства съёма информации к телефонной линии

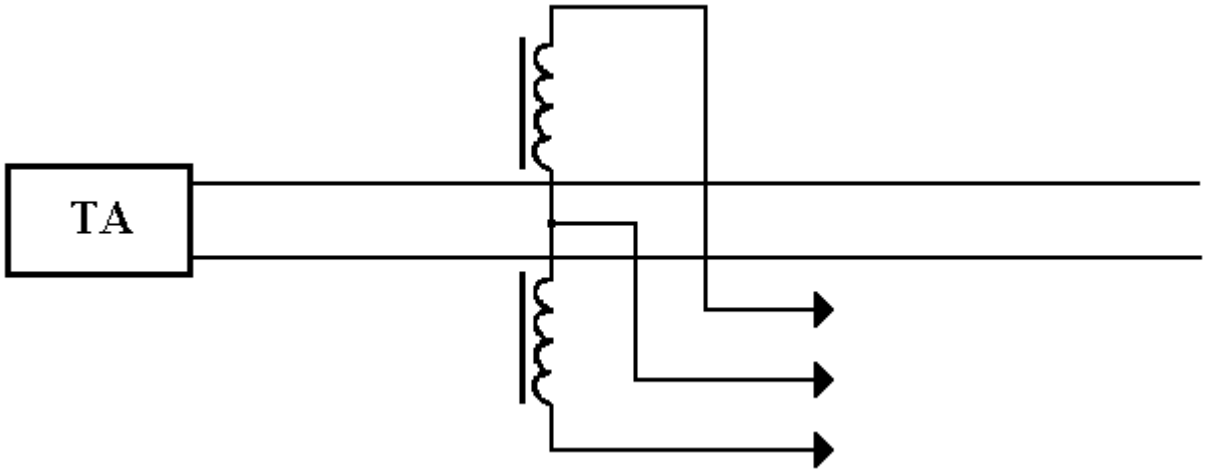

Рисунок 2.3 – Бесконтактное подключение устройства съёма информации к телефонной линии

– Телефонные закладки

Телефонные закладки подсоединяются в абсолютно любом месте телефонной линии и имеют почти вечный срок службы, потому что питаются от контролируемой сети. Большинство телефонных закладок автоматически активируются, когда пользователь снимает трубку, а затем передают по радиоканалу телефонный разговор на пункт перехвата, где его могут записать и затем прослушать. Данные устройства используют микрофон самого телефона и у них отсутствует собственный источник питания, что позволяет делать их весьма маленькими.

– Перехват побочных электромагнитных излучений и наводок

Любое электронное устройство при своей работе создает побочные электромагнитные излучения и наводки (ПЭМИН). При наборе номера и ведении разговоров, из-за технических особенностей блока питания, вся информация излучается на десятках частот в СВ, КВ и УКВ диапазонах. Такое излучение может быть зафиксировано на расстоянии до 200 м.

Таким образом, существующая уже не одно десятилетие традиционная телефония, без которой современный бизнес не может существовать, увы, не обеспечивает достаточный уровня защиты передачи информации, которая ей доверяется. Разумеется, можно использовать различные «навесные» системы защиты – нейтрализаторы, блокираторы и скремблеры, но в этом случае соответственно повышается стоимость системы домашней телефонии. Гораздо более эффективным решением является использование инфраструктуры IP-телефонии. При этом защитные функции уже встроены во все компоненты IP-телефонии, начиная от телефонов и заканчивая серверами управления.

Глава 3. Способы защиты смарт-станции

3.1 Организация защиты передачи сигналов по беспроводным сетям WLAN (беспроводная локальная сеть).

3.1.1 Способы организации передачи управляющих сигналов при помощи сетей WLAN.

Сеть WLAN – это один из типов локально-вычислительной сети (LAN), который использует для связи и передачи данных между какими-либо узлами высокочастотные радиоволны. Представляет собой гибкую систему передачи данных, которую можно применить в качестве расширения, или альтернативы проводной локальной сети внутри одного дома или в пределах какой-либо зоны.

Хотелось бы рассказать о преимуществах использования WLAN за место кабельной локальной сети:

- Увеличение продуктивности. Сеть WLAN предоставляет не привязанную к конкретным помещениям сеть и доступ в Internet. Сеть WLAN дает пользователям возможность передвигаться по территории предприятия или организации, и при этом быть подключенными к сети.
- Быстрое и простое построение локальной сети. Нет необходимости протягивать и закреплять кабели.
- Гибкость установки. Беспроводную сеть без проблем можно установить там, где нельзя провести кабели; технология WLAN делает проще временную установку сетки и ее перемещение.
- Пониженная стоимость использования. Беспроводные сети понижают цену установки, так как не требуются проводные

соединения. Вследствие этого достигается экономия, настолько более значительная, насколько чаще меняется место использования.

– Масштабируемость. Увеличение объёма и перенастройка сети для WLAN не представляет собой сложную задачу: пользовательские устройства возможно объединить в сеть, поставив на них беспроводные сетевые адаптеры.

– Совместимость. Разнообразные марки совместимых клиентских и сетевых устройств могут взаимодействовать друг с другом.

Радиус действия радиочастот, особенно в помещениях, напрямую зависит от характеристик изделия (также и от мощности передатчика), устройства приемника, помехозащищенности и линии прохождения сигнала. Взаимодействие радиоволн со стандартными объектами в здании, такими как стены, металлические конструкции и даже люди, вполне может оказать влияние на дальность распространения сигнала, и из-за этого, изменить охват действия конкретной системы. Беспроводные сети используют радиочастоты, так как радиоволны в помещениях проходят через перекрытия и стены. Зона обхвата систем WLAN с наиболее простыми антеннами может достичь трёхсот метров, а если в распоряжении имеются антенны с большим усилением – до семи километров, в зависимости от видов препятствий и их количества. При помощи дополнительных точек доступа появляется возможность расширить зону охвата, и тем самым дать свободу передвижения.

Функционирование сетей WLAN регламентировано стандартами IEEE 802.11. Исключительно в этих стандартах определяется порядок организации

беспроводных сетей на уровне доступа к среде передачи данных (MAC-уровень) и на физическом уровне (PHY-уровень).

Наиболее простой структурой построения WLAN-сети считается соединение «точка-точка». Узлы сети напрямую связаны друг с другом. Эта структура весьма удобна для быстрого развертывания сетей, однако не подходит для выполнения поставленной цели – построения защищенного информационного обмена с объектом, потому как данная топология нужна для развертывания временных сетей, огромное количество узлов соединять по данной схеме непрактично и неудобно.

Поэтому за основу можно взять другой вид организации беспроводных сетей, который называется Infrastructure Mode – инфраструктурный режим.

В данном режиме узлы сети связаны между собой не напрямую, а через точку доступа – Access Point. Инфраструктурный режим представляет собой объединение сразу нескольких точек доступа, в данном случае точки доступа имеют возможность взаимодействовать друг с другом, а пользователь способен переходить от одной точки доступа к другой.

Пользовательские устройства можно объединить в сеть, поставив на них беспроводные сетевые адаптеры. Наиболее важным элеменом беспроводных сетей является беспроводная точка доступа.

Точки доступа могут выполнять самые разные функции, как для подключения нескольких компьютеров (каждый с беспроводным сетевым адаптером) в самостоятельные отдельные сети, так и для выполнения функции моста между проводными и беспроводными зонами сети.

3.1.2 Организация защищенного обмена при использовании WLAN технологии и построение структурной схемы защищенного обмена

Стандарт RadioEthernet IEEE 802.11 – является стандартом организации беспроводных коммуникаций на определённой территории в режиме локальной сети, это когда у нескольких абонентов есть равноправный доступ к общему каналу передач. Также это 1-ый промышленный стандарт для беспроводных локальных сетей (Wireless Local Area Networks или WLAN).

Стандарт IEEE 802.11 предусматривает определённые средства защиты беспроводных сетей:

- Контроль доступа по имени сети (ESSID). Используется уникальный код ESSID, что идентифицирует сеть.
- Авторизация и аутентификация пользователя
- Контроль доступа по MAC-адресам в беспроводной сети. На точку доступа можно разрешить или запретить авторизацию
- Использование ключей SSID (Service Set Identifier): каждому легальному пользователю сети необходимо получить от администратора особый уникальный идентификатор сети
- Шифрование трафика по протоколам WPA и WPA2.

Самым трудным моментом при установке беспроводной сети является настройка точки доступа. Важно не только купить и установить хорошую точку доступа, но (и это главное) грамотно ее настроить. Каждая точка имеет собственный, особый MAC-адрес, с его помощью она и обнаруживается в локальной проводной сети. Настройку точки доступа можно осуществлять при помощи специальных утилит, вэб-интерфейса, протокола Telnet.

Принцип работы WLAN подразумевает, что информация передается беспроводным способом с помощью радиоволн. Конечно, находясь в зоне действия сети, возможно перехватить эту информацию, если настроится на определенную частоту. Поэтому безопасность в беспроводной сети считается

не менее важным критерием, чем скорость передачи данных. Все нынешние Wi-Fi-устройства поддерживают стандарт шифрования WPA.

При настройке беспроводной сети основное внимание нужно обратить на безопасность. Необходимо непременно включать шифрование WPA, а также желательно прописывать списки доступа клиентов, так как, большинство успешных попыток взлома сетей Wi-Fi происходит из-за халатности.

Также при подборе точки доступа надо принять к сведению функциональное наполнение модели, так как существует большое количество точек, которые могут объединять в себе несколько устройств, как, к примеру, мост, роутер, повторитель, принт-серв. и т.д. Перед покупкой точки доступа, необходимо иметь понятие о том, какие задачи она должна выполнять.

Чтобы визуально представить сеть WLAN в автономном объекте, на рисунке 3.1 изображена типовая незащищённая структурная схема организации информационного обмена данными с объектом при помощи беспроводных сетей.

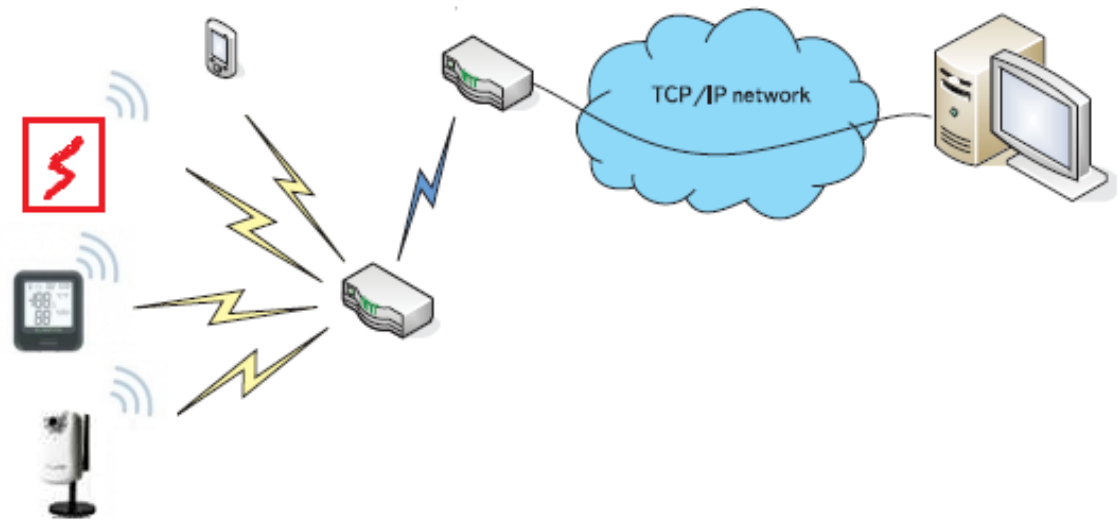

Рисунок 3.1 – Типовая структурная схема беспроводной сети

При выборе модели беспроводного устройства сначала стоит обратить внимание не на его производителя, а на функциональные возможности устройства. Если говорить о простейшей точке доступа, то под функциональностью подразумевается поддержка ею тех или иных протоколов связи и их комбинации. Помимо этого, важными факторами можно назвать поддерживаемые ею протоколы шифрования и аутентификации пользователей, и возможность использования точки доступа в режиме «мост» для построения рассредоточенной беспроводной сети со множеством точек доступа.

Для обеспечения защиты беспроводной сети, организованной на объекте для передачи управляющих сигналов элементам управления объекта, можно модифицировать структурную схему построения WLAN сети, используя следующие меры:

- Внедрить системы предотвращения вторжений в сеть (Intrusion Prevention System, IPS) — программная/аппаратная система сетевой и компьютерной безопасности, которая обнаруживает вторжения или нарушения безопасности и автоматически защищает от них. IPS способен пропускать трафик через себя на скорости канала, то есть не снижать скорость передачи данных. Система IPS гарантирует сборку передаваемых пакетов в нужном порядке и анализирует эти пакеты для обнаружения следов несанкционированной активности. Во время анализа применяются разнообразные методы обнаружения атак: сигнатурный и поведенческий, а также распознавание аномалий в протоколах. Система IPS может блокировать вредоносный трафик. Система IPS становится составной частью роутера и получает доступ к анализируемому трафику моментально после поступления его на определенный интерфейс.

– Использование особых опций в беспроводных роутерах для сокрытия имени сети (возможность сделать сеть невидимой), фильтрация устройств по MAC-адресу. Точки доступа обычно даются со стандартным именем сети, транслирующиеся клиентам, для рекламы наличия этой точки доступа. Необходимо изменить это сразу же после установки. При переименовании SSID точки доступа нужно выбрать такое название, которое непосредственно не относится к вашей компании. Также необходимо настроить сеть таким образом, чтобы доступ был только у определённых устройств, а остальные в сеть не допускались. Для этого существуют фильтры по MAC-адресам устройств. У любого сетевого устройства, помимо IP-адреса, по которому его можно увидеть в сети, и который можно менять в разных сетях (другими словами, у ноутбука дома один IP-адрес,на работе — другой, в кафе с бесплатным WiFi — третий и т.д.), есть ещё и MAC-адрес, который присваивается устройству производителем и, обычно, не меняется. Вот по нему и можно отфильтровать все «нужные» устройства, а все остальные — запретить. Раздел конфигурации роутера или точки доступа называется «MAC Filtering». В нём можно создать список разрешённых и запрещённых MAC-адресов.

– Использование межсетевых экранов. Это комплекс аппаратных и программных средств в компьютерной сети, который осуществляет контроль и фильтрацию проходящих через него IP-пакетов в соответствии с установленными правилами, они выполняют, в первую очередь, свою основную функцию — фильтруют пакеты, не соответствующие определённым в настройках параметрам.

– Введение ограничений на количество пропускаемых пакетов ICMP и SYN на интерфейсах роутеров. Данная мера защищает нашу сеть от DOS атаки

– Использование системы отслеживания «чужих» устройств. Физическое устранение несанкционированных устройств это важный этап снятия угрозы со стороны беспроводных сетей. Однако найти точное местоположение устройства не всегда так просто. Обычно, с портативными анализаторами нужно ходить по всей площади покрытия, чтобы обнаружить «нежелательное» устройство. Однако, нынешние WIPS могут обеспечить точное отслеживание местоположения на конкретном этаже для быстрого устранения «нежелательных» устройств. Система (WIPS) контролирует спектр радиочастот на наличие посторонних, точек доступа и использования беспроводных средств нападения. Система контролирует радио спектр беспроводных локальных сетей, и моментально предупреждает сисадмина о посторонней точке доступа. Обычно это достигается путем сравнения MAC-адресов из участвующих беспроводных устройств.

  – Физическая безопасность точек доступа. Точки доступа должны быть закрыты от прямого вмешательства или кражи. Если это возможно, их необходимо размещать над подвесным потолком, таким образом, чтобы была видна только антенна. В случае отсутствия такой возможности, управление через последовательный порт необходимо отключить и сделать доступным только через безопасные методы доступа.

3.2 Организация защиты передачи управляющих сигналов по средствам проводной телефонной линии.

3.2.1 Способы организации передачи управляющих сигналов при помощи проводной телефонной линии.

Телефонная сеть общего пользования (ТфОП) использует обычные проводные телефоны и оборудование для передачи данных. Сеть предусматривает наличие мини-АТС (специализированного компьютера), в которую входят внешние телефонные линии, а из нее разводятся линии внутренней связи. Такая сеть представлена на рисунке 3.2.

Проводная телефонная линия развертывается в соответствии с ГОСТ 5238-81 «Установки проводной связи. Схемы защиты от опасных напряжений и токов, возникающих на линиях» [10]. Настоящий стандарт распространяется на станционные и линейные установки сетей междугородной, городской, сельской и железнодорожной телефонно-телеграфной связи. Также он устанавливает основные технические требования к схемам защиты установок проводной связи от опасных напряжений и токов, которые возникают на линиях связи при грозовых разрядах, и других импульсных воздействиях, а также при опасном влиянии линий электропередачи и соединении проводов линий связи с проводами линий электропередачи напряжением до 600В, технического персонала и абонентов от акустических ударов.

Телефонный аппарат функционирует по принципу симплексной и дуплексной связи.

Симплексный способ: Разговор между абонентами происходит по схеме 'говорю-слушаю' – абоненты передают информацию по очереди, каждый из них, перед тем как начать говорить, должен нажать кнопку на телефонной трубке для передачи сообщения.

Дуплексный способ: разговор абонентов в реальном времени, то есть позволяет и говорить, и слушать одновременно.

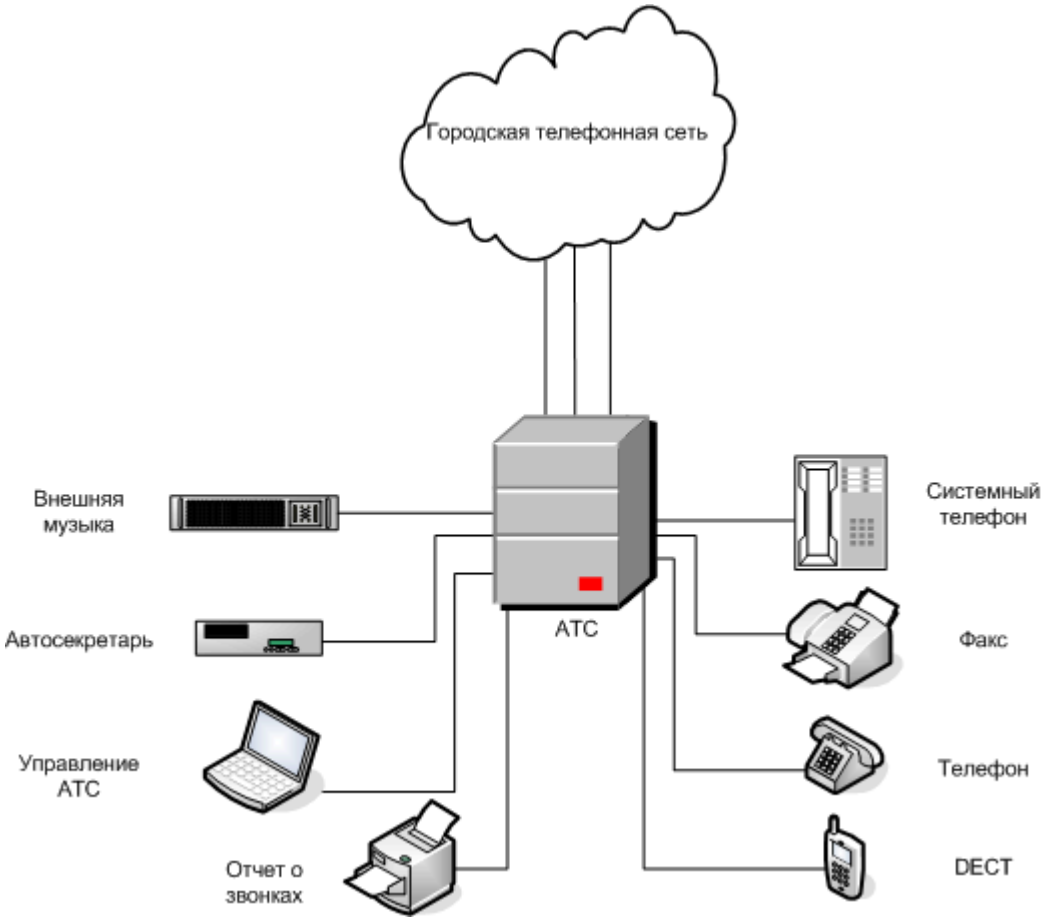

Рисунок 3.2 – организация проводной телефонной линии АТС.

Как видно из рисунка использование АТС при развертывании проводной телефонной линии на объекте является оптимальным решением для малого и среднего офиса.

Таким образом, мини АТС – это:

- телефон (городской и внутренний) на одном устройстве;
- возможность быстрой обработки исходящих и входящих звонков, а также удобная система переадресации;
- наличие большого количества дополнительных сервисных функций, что позволяют использовать связь с максимальным удобством;
- построение собственной корпоративной сети;
- возможность получения современных услуг связи по высокоскоростным каналам передачи данных;

Современные цифровые АТС имеют широкий набор функций — от возможностей аналоговых АТС до организации полностью цифрового канала связи, если абоненты используют цифровые системные телефоны, работающие в двухпроводном режиме. Цифровая АТС – представляет собой современную телестанцию, в которой управление и коммутация полностью цифровые. Это позволяет бесконечно расширять перечень ее функций и возможностей. Сигнал, который исходит от первоисточника, оцифровывается, а затем передаётся внутри АТС и между ними в цифровом виде. Это минимизирует помехи и является гарантией отсутствия затухания, при этом путь длины сигнала может быть любым. Универсальность цифровых АТС состоит в том, что при изменении конфигурации программного обеспечения есть возможность создавать системы с большим набором функций, в зависимости от требований и нужд клиента.

3.2.2 Организация защищенного обмена при использовании проводной телефонной линии и построение структурной схемы защищенного обмена

Телефонную систему связи можно представить в виде нескольких условных зон, показанных на рисунке 3.3 [14].

Зона «А»: к ней относится телеф. аппарат абонента (ТА).

Зона «Б»: Сигнал от ТА по телефонному проводу попадает в распределительную коробку (РК).

Зона «В»: из РК сигнал попадает уже в магистральный кабель.

В каждой зоне имеются свои особенности по перехвату информации, но принципы, на которых построена техника несанкционированного подключения, мало отличаются.

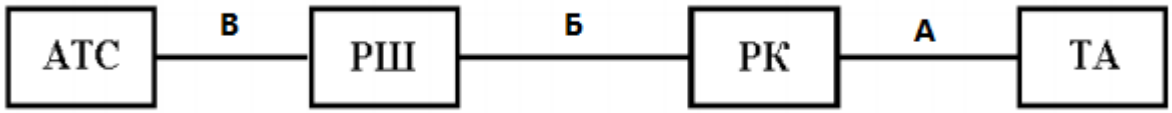

Рисунок 3.3 - элементы сети АТС-абонент

Обнаружение подслушивающих устройств начинается с осмотра телефонных линий и телефонного аппарата (ТА), но эта проверка, возможна только на участке от ТА до РК. Контроль в оставшихся зонах почти невозможен без привлечения служащих АТС. Однако, в связи с тем, что подключения чаще всего и осуществляются в зоне «А», то обнаружить прослушку или следы её применения при хорошем внимании весьма вероятно. При проведении осмотра жизненно необходимо разобрать телефонный аппарат и телефонные розетки. На рисунке 3.4 [14] показан пример внешнего вида «жучка», вмонтированного в ТА. Устройство такого типа может устанавливаться очень быстро и таким способом пользуются только тогда, когда нет времени на более основательное внедрение.

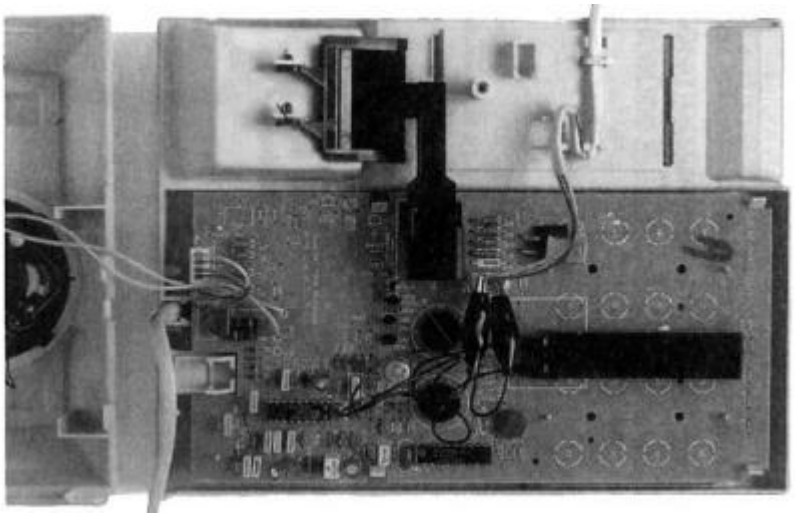

Рисунок 3.4 - Устройство съёма информации, установленное в ТА

Для того, чтобы обеспечить защиту информации, что идёт по телефонным линиям связи, требуется спец аппаратура. Её по принципу действия можно разделить на несколько групп.

Аппаратура контроля линий связи:

- Индикаторные устройства;
- Анализаторы проводных линий и кабельные локаторы (последние, делятся на два типа: рефлектометры и устройства, которые используют принципы нелинейной локации);
- Детекторы поля, специальные радио приемные устройства и особые комплексы контроля.

Аппаратура защиты:

- Многофункциональные устройства защиты телефонных линий;
- Устройства ликвидации «закладок»;
- Устройства защиты от несанкционированного подключения;
- Аппаратура пространственного и линей ного зашумления;
- Аппаратура кодирования информации;
- Аппаратура защиты от ВысЧаст-навязывания.

Выбор аппаратуры контроля за несанкционированным подключением к проводной линии связи.

Выбранным индикатором наличия подслушивающих устройств является устройство типа ЛСТ-1007, обычно называемое «Телефонный страж», представленное на рисунке 3.5 [14].

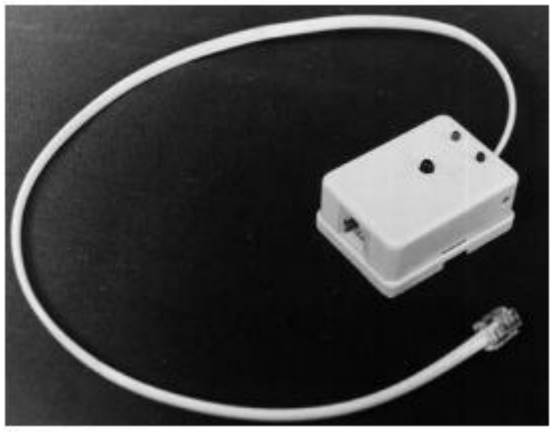

Рисунок 3.5 - Телефонный страж, ЛСТ-1007

Это устройство устанавливается на уже проверенной телефонной линии и настраивается в зависимости от её параметров. Питание идёт от самой линии. При подключении любых несанкционированных устройств, что тоже питаются от телефонной сети (например, аппаратура с непосредственным включением), подается сигнал тревоги (горит красная лампочка).

Для более тщательного анализа телефонной линии на предмет утечек информации нужно проводить систематические проверки, используя для этого специальные анализаторы телефонных линий. В качестве примера могу привести анализатор телефонной линии, представленный на рисунке 3.6 [14], ВИЗИР – низкочастотный нелинейный детектор проводных коммуникаций, рассчитан для выявления средств прослушки, что могут быть подключены к

проводным коммуникациям (силовые, слаботочные) для съема и передачи информации, а также к цепям питания подобных устройств. Принцип действия прибора заключается в следующем: в линию подаются зондир. синусоидальн. сигнал и регистрируются высшие гармоники тока, что возникают в полупроводниковых элементах подсоединённого к линии средства прослушки. Анализ наличия высших гармоник оператор проводит путём наблюдения за изображением на ЖК-экране прибора.

Рисунок 3.6 - Анализатор телефонных линий ВИЗИР

Выбор аппаратуры защиты от несанкционированного подключения к проводной линии связи.

Существует длинный ряд достаточно сложных индивидуальных устройств защиты Тел.Апп., которые выполняют следующие функции:

- изменяют напряжение в линии, что приводит к выключению диктофонов функцией автовключения при снятии трубки и др. устройств, что используют для работы напряжение тел. линии;
- генерируют маскирующую речь помехи, что не мешают разговору, так как они автоматически фильтруется на всех АТС, но при этом те, кто подключился на линию до станции услышат только громкое шипение;
- защищают ТА от попыток модификации с целью использования его для прослушивания помещения.

В качестве примера приведу устройство защиты ТА «БАРЬЕР-3»

«БАРЬЕР-3» – устройство защиты телефонных переговоров, изображёно на рисунке 3.7. Предназначено для защиты телеф. переговоров на участке от ТА до АТС и обеспечивает:

- подавление подслушивающих устройств, что подключены к телеф. линии, независимо от их типов и способов подключения;
- подавление автоматических устройств звукозаписи, что подключены к телеф. линии и активируемых поднятием трубки;
- подавление устройств звукозаписи с ручным управлением записи;
- запуск диктофонов, которые активируются голосом, при положенной трубке;
- защиту от ВысЧаст-навязывания и «микрофонного эффекта», что позволяют прослушивать акустику в помещении через Тел.Апп. с положенной трубкой;
- блокирование работы микрофонов, что работают по телефонной линии;
- блокирование работы параллельного ТА, что подключён к телефонной линии;
- цифровую информацию о напряжении телеф. линии и напряжении отсечки;
- возможность подключения к телеф. линии устройств для звукозаписи для архивации телефонных разговоров.

Рисунок 3.7 - устройство защиты телефонных переговоров «БАРЬЕР-3»

Для практического решения проблем защиты информации нашли применение устройства, которые называют «телефонные киллеры». Принцип их действия основан на подаче высоковольтного напряжения в телеф. линию,

в результате чего уничтожаются все подключенные устройства. В качестве примера приведу выжигатель телефонных закладных устройств «Кобра», представленный на рисунке 3.8 [14]. Он специализирован для предотвращения прослушки абонентских телефонных линий при помощи устройств несанкц. доступа, что устанавливаются в телефонные линии с непосредственным параллельным или последовательным подключением. Принцип работы – это электрическое уничтожение/ выжигание.

Рисунок 3.8 - выжигатель телефонных закладных устройств «Кобра»

Техн. средства пространственного зашумления используются для маскировки информативных побочных электромагнитных излучений и наводок персональных ЭВМ и периферийных устройств, а также другой оргтехники посредством создания помех в широкой полосе частот (как правило, от 1 до 1000 МГц). В качестве устройства защиты от ПЭМИН выбран ГШ-1000 – стационарный генератор шума, представленный на рисунке 3.9 [14]. Обеспечивает маскировку побочных электромагнитных излучений устройств вычислительной техники, размещенных на площади 40 кв. м. Устройство имеет индикацию контроля работоспособности, оборудовано разъемом для подключения внешнего контрольного или управляющего устройства, позволяющего автоматически блокировать работу периферийных систем вычислительной техники в случае возникновения неполадок в работе генератора.

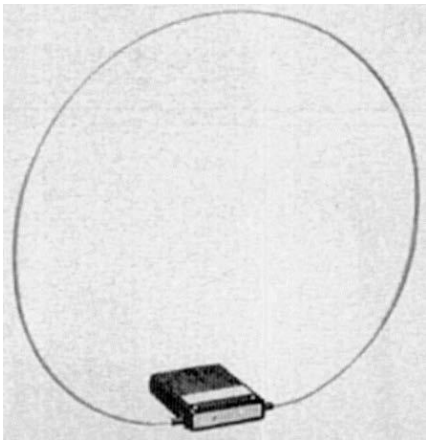

Рисунок 3.9 - стационарный генератор шума ГШ-1000

При физическом нарушении телефонной линии, например, злоумышленник отрезает телефонный кабель, необходимо организовать резервирование линии связи. Достигнуть это можно применив IP АТС, которая позволяет соединить ТФОП, GSM,VOIP сети, посредством оцифровки аналогового сигнала.

Помимо анализа телефонной линии на перехват информации, внедрения радиозакладок и средств прослушивания; помимо резервирования телефонной линии посредством использования IP АТС, необходимо задействовать криптографические методы защиты информации [14].

Для обеспечения криптографической защиты информации в проводных телефонных линиях мною выбран метод скремблирования. Этот метод заключается в объединении временных перестановок в передаваемом сообщении и частотной перестановке (инверсии) в спектре передаваемого сигнала. При этом временные манипуляции разрушают смысловой строй, а частотные преобразования перемешивают гласные звуки.

Устройства, что реализуют вышеописанные операции, носят название аналоговых скремблеров. При выборе устройств данного типа необходимо обратить внимание в первую очередь на сложность преобразований, что применены в нём, а не на число возможных ключевых комбинаций.

Приведу в пример скремблер «Орех-А», представленный на рисунке 3.10 [14]. Прибор не особо бросается в глаза, так как выполнен в виде

подставки под телеф. аппарат и обладает всего одной кнопкой. Это изделие смело может претендовать на оценку одного из лучших отечественных приборов данного типа по параметру стоимость/эффективность.

Рисунок 2.16 - Скремблер «Орех-А»

Таким образом, сформировав все выбранные методы защиты проводной телефонной линии можно построить структурную схему защищенного информационного обмена телефонной линии.

Глава 4.Безопасность жизнедеятельности.

4.1 Вредные и опасные производственные факторы.

В процессе трудовой деятельности на сотрудника офиса могут воздействовать опасные (вызывающие травмы) и вредные (вызывающие заболевания) произв. факторы.

К вредным и опасным физическим факторам относятся:

-движущиеся части любого офисного оборудования (к примеру - каретка принтера);

-повышенный уровень пыли и газа в воздухе в рабочей зоне;

-повышенная температура поверхностей офисной техники;

-повышенный уровень ЭМ излучений;

-повышенная или пониженная темп. воздуха в рабочей зоне;

-повышенная или пониженная влажность воздуха;

-повышенная или пониженная подвижн. воздуха;

-повышенный уровень шумов на рабочем месте;

-повышенная ионизация воздуха;

-повышенный уровень ионизир. излучений;

-повышенное напряжение в электрич. цепи;

-повышенный уровень статич. электричества;

-повышенная напряженность магн. поля;

-малая освещенность в рабочей зоне;

-отсутствие или недостаток естественного света.

Применительно к офисным помещениям химические факторы можно представить повышенным уровнем озона, наличием формальдегидов в офисной мебели и т.д.

К биологическим вредным и неблагоприятным производственным факторам относятся какие-либо микроорганизмы (бактерии, вирусы и др.), воздействие которых на работников вызывает заболевания и/или травмы.

К психофизиологическим опасным и вредным производственным факторам можно отнести нервно-психические перегрузки (эмоциональное и умственное перенапряжение, перенапряжение анализатора слуха, зрения и др.).

Уровни воздействия на работающих неблагоприятных производственных факторов нормированы предельно-допустимыми уровнями, значения которых указаны в соответствующих стандартах системы стандартов безопасности труда и санитарно-гигиенических правилах.

4.2 Степень воздействия офисной техники на сотрудников.

Ниже рассмотрена офисная оргтехника и степень ее воздействия на работника.

4.2.1.Персональный компьютер. (ПК)

Основные опасные и неблагоприятные производственные факторы, которые воздействуют на человека при работе с перс. компьютером, следующие:

- повышенный уровень ЭМ излучений;
- повышенный уровень ионизир. излучений;
- повышенный уровень статич. электричества;
- повышенная напряженность электростатич. поля;
- повышенная или пониженная ионизация воздуха;
- повышенная яркость света;
- статические перегрузки костно-мышечного аппарата и динамические перегрузки мышц кистей рук;
- перенапряжение зрения;
- умственное перенапряжение;

-эмоциональные перегрузки;

-монотонный труд.

К вредным излучениям компьютера можно отнести низкочастотные электромагнитные поля и ионизирующее (рентгеновское) излучение мониторов на электронно-лучевых трубках (ЭЛТ). Что по поводу электромагнитных полей, то их влияние на человека изучено слабо, а уровень этого излучения от ПК очень низкий, даже если сравнивать со многими другими бытовыми электроприборами. Однако многочисленными исследованиями доказана возможность нарушения протекания беременности при долгой работе женщин за компьютером. Помимо этого, установлено, что долгое пребывание детей в зоне воздействия низкочастотных магнитных полей повышает вероятность появления у них опухолей мозга. Именно в связи с этим существуют некоторые ограничения по размещению компьютеров в помещении, а также по допуску персонала к работе за перс. компьютером.

У приборов на ЭЛТ есть еще один вредный фактор: технология получения изображения в них сопряжена с использованием высоких напряжений

в несколько десятков Квольт, необходимых для формирования электр. лучей. Побочным эффектом этой технологии является увеличение концентрации положительно заряженных ионов в воздухе и снижение числа отрицательных ионов (плюс увеличение концентрации озона), что может неблагоприятно сказывается на самочувствии и здоровье человека. Хотя официальная медицина пока что не уделяет этому фактору особого внимания, все же СанПиН регламентирует уровень содержания положительных и отрицательных ионов в воздухе помещений с ПЭВМ. В любом случае, массовый переход на ЖКИ-мониторы избавляет пользователей от этого, возможно, вредного фактора.

Работа на перс. компьютерах можно отнести к зрительно напряженным работам, что значит, что именно глаза страдают в первую очередь при работе с Перс. компьютером. Именно этот вредный фактор описан в большинстве документов, регламентирующих труд работников с использованием ПЭВМ. Необходимо понимать, что неблагоприятное воздействие на глаза проявляется не в присутствии каких-либо излучений, а в необходимости непрерывного напряжения глаз при считывании информации с экрана. Поэтому для профилактики отрицательных воздействий нужно соблюдать установленный режим работы и отдыха.

На утомление глаз довольно ощутимо влияет уровень освещенности рабочего места. Особенно это заметно при необходимости одновременной работы как с электронными , так и с бумажными документами. Согласно СанПиН, уровень освещенности рабочего места при работе на компьютере должен составлять 300-500 лк. При этом монитор и источники освещения должны быть расположены таким образом, чтобы не формировать блики на поверхности экрана.

Поскольку экран монитора – это тоже источник света, при непрерывном чтении информации с него происходит довольно быстрое утомление глаз, в особенности если яркость свечения монитора установлена очень высокой. Также раздражение глаз обычно вызывает мерцание изображения на мониторе из-за низкой частотой кадровой развертки. Для того, чтобы снизить мерцания экрана рекомендуется установить частоту кадров не менее 75 Гц для ЭЛТ-мониторов. В силу технологических особенностей для ЖКИ-мониторов достаточной является минимальная частота кадров в 60 Гц.

Статичная и напряженная поза при долгой работе за компьютером обычно приводит к воспалению мышц, связок и сухожилий спины и ног, а также заболеваниям позвоночника и суставов (остеохондроз, артрит, артроз и пр.), а постоянное напряжение рук – к повреждениям запястья и сухожилий (к

примеру, синдром лучезапястного сустава). Эти заболевания вызываются травмами повторяющихся нагрузок и являют собой постепенно накапливающиеся недомогания, что обусловлены продолжительными повторяющимися воздействиями и перетекающие в болезни нервов, мышц и сухожилий. Влияние этого вредного фактора можно снизить, если правильно организовать рабочее место – оптимально подобрать мебель и правильно разместить элементы и части компьютера.

4.2.2. Принтер.

Если работа с ПК во многом регламентирована законодательно, то этого нельзя сказать о другом оборудовании, которое используется в офисе. Что касается принтера, то его использование не требует постоянного нахождения работника, напряжения внимания и т.п. Всю работу с принтером можно свести к его включению и выключению, добавлению бумаги и изыманию отпечатков. А замену картриджей чаще всего выполняет не пользователь, а кто-либо из обслуживающего персонала.

Несмотря на это любой принтер представляет собой сложный электроприбор, поэтому при работе с ним нужно выполнять стандартные требования к пожарной и электробезопасности. Также в любом принтере имеются движущиеся части, а некоторые элементы нагреваются в процессе работы до высокой температуры (в матричных и струйных принтерах - печатные головки, в лазерных принтерах – специальные нагревательные валы).

Другим вредным фактором при работе с принтерами может являтся шум. Наибольшем уровнем шума во время работы обладают матричные принтеры, однако в паспортах этих приборов уровень шума, как правило, не указан, а фактический уровень может быть измерен разве что при проведении аттестации рабочего места.

Это единственный тип принтеров, уровень шума которых может быть сопоставим с максимально допустимым на рабочих местах, оборудованных ПЭВМ. Все остальные принтеры работают заведомо тише.

4.2.3 Телефон

Трудно представить себе какую-либо опасность, которую может представлять привычный всем стационарный телефон или факс аппарат. Действительно, телефон прост и безопасен в эксплуатации. Однако не многим известно, что напряжение в телефонной линии может достичь достаточно больших величин. Например, при входящем звонке, согласно стандартам, которые действуют на территории стран СНГ, напряжение в телефонной линии может составлять до 120 В переменного тока.

Факс аппараты вообще подключаются к сети переменного тока 220 В и требуют обязательные соблюдения соответствующих мер по безопасности.

В отличие от стационарных аппаратов, мобильн. телефоны не являются столь же безопасными. Любой мобильный телефон является источником высокочастотного ЭМ излучения. Его воздействие на ткани человеческого тела аналогично воздействию излучения, которое применяется в микроволновых печах. Естественно мощность излучения телефона гораздо меньше, но оно тоже способно приводить к локальному нагреванию живых тканей, разрывам молекул ДНК и другим повреждениям клеток организма. В связи с этим российские гигиенические требования настоятельно рекомендуют ограничить использование мобильных телефонов лицами, не достигшими 18 лет, а также беременных женщин и тех, у кого имплантирован водитель сердечного ритма.

4.3 Меры по снижению вредного воздействия

4.3.1 Окраска и коэффициенты отражения

Окраска помещений и мебели обязана способствовать созданию благоприятных условий для зрительного восприятия и хорошего настроения.

Источники света, коими могут являться светильники и окна, дающие отражение от поверхности экрана, значительно ухудшают точность знаков и могут повлечь за собой помехи физиологического характера, которые выразятся в значительном напряжении, особенно при продолжительной работе. Отражение, + включая отражения от вторичных источников света, должно быть сведено к минимуму. Для защиты от избыточной яркости окон могут быть повешены шторы и экраны.

В зависимости от расположения окон рекомендуется следующая окраска полов и стен:

Если окна расположены к югу: - стены зеленовато-голубого или светло-голубого цвета; пол - зеленый;

Если окна расположены к северу: - стены светло-оранжевого или оранжево-желтого цвета; пол - красновато-оранжевый;

Если окна расположены к востоку: - стены желто-зеленого цвета;

пол зеленый или красновато-оранжевый;

Если окна расположены к западу: - стены желто-зеленого или голубовато-зеленого цвета; пол зеленый или красновато-оранжевый.

В помещениях, где находится ПК, нужно обеспечить следующие цифры коэфф-та отражения:

-для потолка: около 60…70%,

-для стен: около 40…50%,

-для пола: около 30%.

-для других пов-стей и рабочей мебели: около 30…40%.

4.3.2 Электробезопасность

Применительно к компьютерной технике нужно учитывать несколько не написанных в типовых инструкциях замечаний:

а) Никогда не вставляйте в привод для оптических дисков CD и/или DVD диски, на которых присутствуют трещины и сколы. Во время работы диск раскручивается до очень большой скорости, и поэтому действующая на него центробежная сила вполне может разорвать дефектный диск в приводе. При этом эффект практически аналогичен взрыву, а кинетич. энергия разлетающихся осколков диска такова, что есть случаи пробоя ими даже металлических частей корпуса ПК.

б) При использовании каких-либо источников бесперебойного питания необходимо помнить, что включенный источник выдает опасное для жизни напряжение в 220 В, даже если он отсоединен от стационарной питающей сети (так как это и есть его основная задача).

в) Во время грозы лучше будет отсоединить разъемы телефонной линии от модема, поскольку в большинстве случаев телефонные линии не имеют защиты от гроз и часто становятся причиной выхода из строя как модемов, так и других частей ПК. То же самое можно отнести к разъемам локальной вычислительной сетки, если у неё есть расположенные снаружи здания участки, которые не оборудованы грозо защитой.

г) Во многих зданиях по сей день используется электр. проводка, которая не имеет отдельного заземляющего провода. Поэтому подключение персональных компьютеров к такой сети может вызвать появление ненулевых потенциалов на корпусе и разъемах системного блока, что может привести к выходу оборудования из строя при присоединении и отсоединении разъемов, а также к возможному удару электр. током в случае касания металических частей корпуса.

Строго говоря, использование компьютеров без заземления запрещено, однако на практике часто ограничиваются установкой розетки с заземляющим контактом, который фактически не заземлен. По этой причине никогда не следует прикасаться к металлическим частям корпуса и разъемов ПК во время его работы,а также к пов-сти экрана ЭЛТ-монитора (на нем накапливается статическое электричество, которому некуда стекать, так как нет заземления), не производите подключение и отключение разъемов при включенном в сеть персональном компьютере.

Известны случаи выхода из строя незаземленных компьютеров даже при присоединении устройств, которые поддерживают так называемое «горячее» подключение (например, устройства с подключением через разъем USB).

Фактически, использование компьютеров без заземления – это грубое нарушение норм охраны труда.

4.3.3 Освещение

Правильно спроектированное и выполненное производственное освещение улучшает условия зрительной работы, а также снижает утомляемость, повышает производительность труда и благотворно влияет на производственную среду, при этом оказывая положительное психологическое воздействие на работника, а также повышает безопасность труда и снижает шанс получения травмы.

Недостаточность освещения может привести к напряжению зрения, ослаблению внимания, что приводит к наступлению преждевременной утомленности. Чрезмерно яркое освещение вызывает ослепление, раздражение и резь в глазах. Ошибочное направление света на рабочем месте может формировать резкие тени, блики, а также дезориентировать работающего. Всё это может привести к несчастному случаю или профессиональным заболеваниям, именно по этой причине правильный расчет освещенности столь необходим и важен.

Освещение делится на три вида - естественное, искусственное и совмещенное (естественное и искусственное вместе)

Согласно СНиП II-4-79 в помещениях офисных центров применяется система комбинированного освещения. Комбинированное освещение - освещение, при котором к общему добавляется ещё и местное освещение.

Помимо этого все поле зрения должно быть освещено достаточно равномерно – это основное гигиеническое требование. Другими словами, степень освещения помещения и яркость экрана ПК должны быть примерно одинаковыми, потому как яркий свет в районе периферийного зрения сильно увеличивает напряженность глаз и приводит к их быстрой утомляемости.

4.3.4 Параметры микроклимата

Вычислительная техника может являться источником существенных тепловыделений, что способно привести к увеличению температуры и уменьшению относительной влажности в помещении. В помещениях, где находятся персональные компьютеры, необходимо соблюдать определеннные параметры микроклимата. В санитарных нормах СН-245-71 расписаны величины параметров микроклимата, которые создают комфортные условия для деятельности. Эти нормы устанавливаются в зависимости от времени года, характера трудового процесса и типа производственного помещения.

Объем помешений не должен быть меньше 19,5м3 на человека при учёте максимального количества одновременно работающих в смену.

Для обеспечения комфортных условий обычно используются как организационные методы (разумная организация проведения работ, зависящая от времени года и времени суток, а также чередование труда и отдыха), так и современные технические средства (вентиляция, кондиционирование воздуха, система отопления).

4.3.5 Шум и вибрация

Шум может ухудшать условия труда, оказывая неблагоприятное воздействие на человеческий организм. Работники в условиях длительного шумового воздействия могут испытывать раздражительность, снижение памяти, головные боли, головокружение, повышенную утомляемость, понижение аппетита, боли в ушах и т. п. Такие нарушения в работе ряда органов и систем человеческого организма могут вызывать негативные трансформации в эмоциональном состоянии человека вплоть до стрессового состояния.

Под воздействием шума снижается концентрация внимания, нарушаются физиологические функции, возникает усталость в связи с увеличенными энергетическими затратами и нервно-психическим напряжением, ухудшается речевая коммутация. Все эти факторы снижают работоспособность человека, производительность, а также безопасность и качество труда. Продолжительное воздействие интенсивного шума (выше 80 дБ) на слух человека может привести к его частичной или полной потере.

Уровень шума на рабочем месте не должен превышать 50дБ. Для того чтобы снизить уровень шума, стены и потолок помещений, где установлены ПК, могут быть облицованы звукопоглощающими материалами, а уровень вибрации в помещениях можно снизить путем установки технического оборудования на специальные вибро изоляторы.

4.3.6 ЭМ и ионизирующее излучение

К основным регламентированным СанПиН нормам, при работе на ПЭВМ необходимо отнести следующее:

- S одного рабочего места, оборудованного ПЭВМ, должна составлять не менее шести кв.м., для электронно-лучевого монитора и четыре с половиной кв.м. для ЖК монитора, объем – не менее двадцати куб.метров. Для исключения влияния повышенных уровней ЭМ излучений расстояние между экраном монитора и работником должно составлять не менее полуметра м (оптимальное 0,6–0,7 м).

- Для того, чтобы обеспечить безопасность работников на соседних рабочих местах расстояние между рабочими столами с мониторами (в направлении тыла поверхности одного монитора и экрана другого монитора) должно составлять не менее двух метров, а расстояние между боковыми поверхностями мониторов – не менее 1,2 м. Женщины со времени установления беременности ,а также в период кормления грудью к работам с использованием ПК не допускаются.

- при интерактивной работе с компьютером устанавливаются следующие регламентированные перерывы:

1)при работе с ПК не более двух часов за смену (первая категория сложности) – два перерыва по 15 минут через два часа после начала смены и через два часа после обеденного перерыва;

2)при работе с компьютером от 2 - х до 4 - х часов за смену (вторая категория сложности) – два перерыва по 15 минут через два часа после начала смены и через 1,5–2 часа после обеденного перерыва, либо перерывы по десять минут после каждого рабочего часа;

3)при работе с компьютером от 4 - х до 6 - и часов за смену (третья категория сложности) – два перерыва по 20 минут через 1,5–2 часа после начала смены и через 1,5–2 часа после обеденного перерыва, либо перерывы по пятнадцать минут после каждого рабочего часа.

Важно, что работа с персональным компьютером в течение более шести часов за одну смену (при восьмичасовой рабочей смене) не

допускается. Также не допускается непрерывная работа за компьютером свыше двух часов. В ночное время суток общая продолжительность регламентированных перерывов для абсолютно всех категорий сложности должна увеличиваться на один час. Для преподавателей длительность работы в комп. классах не должна превышать четыре часа в день. Во время регламентированных перерывов рекомендуется выполнять специальные упражнения для глаз,чтобы снизить напряжение и усталость.

4.3.7 Статическое электричество

Статическое электричество может отрицательно влиять как на человеческий организм, так и на электроприборы.

В ряде случаев электростатический разряд способен вызывать болевые и нервные ощущения и может стать причиной непроизвольного резкого движения, из-за которого человек может получить травму (ушиб, падение и т.п.). Кроме мучений, связанных с ухудшением здоровья людей, что уже непозволительно, это может привести к неблагоприятным экономическим последствиям для фирмы или предприятия в целом.

Электризация материалов часто препятствует нормальному ходу техно логических процессов на производстве, в том числе может создать дополнительную пожарную опасность вследствие образования искры при разрядах при наличии в помещении горючих веществ.

Так называемый "Статический сезон", обычно длится с октября по март. Это период, для которого характерны низкая влажность и температура. Однако, в современных помещениях, которые оборудованы системами климат контроля и кондиционерами, статическое электричество может являться стабильной проблемой. Особенно, в помещениях, в которых находится компьютерное оборудование.

Загрязнения еще больше уменьшают проводимость поверхностей, что также может поспособствовать образованию заряда, который может перейти на человека, не имеющего электрической изоляции (к примеру, носящего кожаную обувку). Проходя через человеческое тело (которое является превосходным проводником), заряд затухает в первой же проводящей поверхности, к которой прикоснулся этот человек, например, в ручке дверной.

Именно по этой причине необходимо обрабатывать поверхности с помощью антистатиков.

4.4 Эргономические требования к рабочему месту

Рабочее место и взаимное размещение абсолютно всех его элементов обязано соответствовать антропометрическим, физическим и психологическим требованьям. Огромное значение также имеет характер работы. В частности, при организации рабочего места необходимо соблюсти следующие основные условия: оптимальное размещение всего оборудования, которое входит в состав рабочего места, также необходимое и достаточное рабочее пространство, которое позволит осуществлять все необходимые движения и перемещения.

Эргономическими аспектами проектирования рабочих мест, являются:

-высота рабочей пов-сти,

-размер пространства для ног,

-требования к расположению документов на рабочем месте (наличие и размеры подставки для документов, возможность всевозможного размещения документов, расстояние от глаз пользователя до экрана монитора, документа, клавиатуры и т.п.),

-характеристики рабочего кресла,

-требования к пов-сти рабочего стола,

-регулируемость частей рабочего места.

Главными элементами(частями) рабочего места являются стол и кресло. Основным рабочим положением считается положение сидя.

Рабочая поза сидя вызывает минимальную утомляемость. Рациональная планировка рабочего места предусматривает конкретный порядок и постоянство размещения предметов, средств труда и документации на рабочем месте. То, что требуется для выполнения работ чаще, естественно должно быть расположено в зоне легкой и быстрой досягаемости рабочего пространства.

Моторное поле – это часть пространства рабочего места. В нём осуществляются различные действия человека.

Максимальная зона досягаемости рук - это часть моторного поля рабочего места, которое ограничено дугами, которые описываются максимально вытянутыми руками при их движении в плечевом суставе.

Оптимальная зона - это часть моторного поля рабочего места, ограниченого дугами, которые описываются предплечьями при движении в локтевых суставах с опорой в точке локтя и с относительно неподвижным плечом.

Оптимальное размещение предметов труда и документации в зонах досягаемости:

ДИСПЛЕЙ - обычно размещается в центре;

СИСТЕМНЫЙ БЛОК - обычно размещается в предусмотренной нише стола;

КЛАВИАТУРА - в зоне перед монитором;

«МЫШЬ» - в зоне справа;

СКАНЕР - в зоне слева;

ПРИНТЕР - обычно находится справа;

ДОКУМЕНТАЦИЯ: нужная для выполнения работы должна находится в зоне легкой досягаемости ладони, а в выдвижных ящиках стола – литература и документация, которой обычно пользуются редко.

Для комфортной работы стол должен удовлетворять следующим условиям:

1)Высоту стола необходимо выбирать с учетом возможности сидеть свободно, в удобной позе и при необходимости опираясь на подлокотники;

2)Нижняя часть стола должна быть сконструирована таким образом, чтобы работник мог удобно сидеть, и не был вынужден поджимать под себя ноги;

3)Поверхность стола должна обладать необходимыми свойствами, которые исключают появление бликов в поле зрения работника;

4)Конструкция стола обязана предусматривать наличие специальных выдвижных ящиков (не менее трёх для хранения документации, листингов, канцелярских принадлежностей и др.).

5)Высоту рабочей поверхности рекомендуется соблюдать в пределах от 680мм до 760 мм. Высота поверхности, на которую устанавливается клавиатура, должна быть около 650 мм.

Большое значение необходимо придать характеристикам рабочего кресла. Поэтому рекомендуемая высота сиденья над уровнем пола находится в пределах от 420 мм до 550мм. Поверхность сиденья должна быть мягкой, передний край закругленный, а угол наклона спинки обязательно должен регулироваться.

Необходимо при проектировании предусматривать возможность разнообразного размещения документов: между монитором и клавиатурой и т.п. Помимо этого, в случаях, когда монитор имеет низкое качество изображения, например заметны мелькания, расстояние от глаз до экрана обычно делают больше (около 700 мм), чем расстояние от глаз до документа (300-450 мм). При высоком же качестве изображения на мониторе расстояние от глаз пользователя до экрана, документа и клавиатуры может быть равным.

Положение экрана определяется:

-расстоянием считывания (0,6…0,7м);

-углом считывания, направлением взгляда на 20 градусов ниже горизонтали к центру экрана, причем экран перпендикулярен этому направлению.

Должна также предусматриваться возможность регулирования экрана:

-по высоте на 3 см;

-по наклону от -10 градусов до +20 градусов относительно вертикали;

-в левую и правую сторону.

Требования к рабочей позе пользователя следующие:

-голова не должна быть наклонена более чем на 20 градусов,

-плечи должны быть расслаблены,

-локти держатся под углом от 80 до 100 градусов,

-предплечья и кисти рук находятся в горизонтальном положении.

Причина неправильной позы пользователей может быть обусловлена такими факторами как:

-отсутствие хорошей подставки для документов

-слишком высокое или низкое положение клавиатуры

-слишком низкое или высокое положение документов

-нет места для того, чтобы удобно положить руки и кисти

-недостаточное пространство для удобного расположения ног.

Для того, чтобы избавиться от указанных недостатков необходимо соблюсти общие рекомендации:

-наличие передвижной клавиатуры

-должны быть предусмотрены специальные приспособления для регулирования высоты стола, клавиатуры и экрана, а также подставка для рук.

Создание благоприятных условий труда для работников и правильное эстетическое оформление рабочих мест на производстве имеет большое значение, как для облегчения труда, так и для повышения его привлекательности, которая безусловно влияет на производительность труда.

Заключение и выводы

Вывод:

В процессе подготовки дипломной работы была исследована смарт-станция Tellus, изучены её возможности и проанализирована работоспособность. Также в процессе исследования смарт-станции, не было выявлено каких-либо конкретных уязвимостей, поэтому я могу дать только общие рекомендации по защите от внешних угроз.

Благодаря универсальному набору функциональных возможностей смарт-станция идеально подходит для использования в небольших офисах и загородных домах, где необходимо максимально просто и быстро обеспечить наличие экономичной телефонной связи с возможностями мини-АТС и доступа в сеть Интернет, организовать локальную сеть и совместный доступ к хранилищу данных.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Белов Е.Б. Основы информационной безопасности. Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. -М.: Горячая линия - Телеком, 2006. - 544с

2.Галатенко В.А. Стандарты информационной безопасности: курс лекций. Учебное пособие. - 2-ое издание. М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2009. - 264 с.

3.Глатенко В.А. Стандарты информационной безопасности / Открытые системы 2006.- 264с

4.Долженко А.И. Управление информационными системами: Учебный курс. - Ростов-на-Дону: РГЭУ, 2008.-125 с

5.Калашников А. Формирование корпоративной политики внутренней информационной безопасности

6.Мэйволд Э., Безопасность сетей. Самоучитель // Эком, 2009.-528 с

7.Семкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И., Основы организационного обеспечения информационной безопасности объектов информатизации // Гелиос АРВ, 2008 г., 192 с

8.Тихонов В.А., Райх В.В., Информационная безопасность. Концептуальные, правовые, организационные и технические аспекты // Гелиос АРВ, 2009г., 528 с

9.Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. :М - ДМК Пресс, 2008. - 544 с

10.Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. - М.: Книжный мир, 2009. - 352 с

11. Ярочкин В.И., Информационная безопасность: учебник для студентов вузов// -М.: Академический проект; Гаудеамус, 2-е изд., 2009 г., 544 с

12. Шапаренко Ю. М., Бескид П. П., Суходольский В. Ю. «Проектирование защищенных информационных систем. Часть 1. Конструкторское проектирование. Защита от физических полей» Учебное пособие. – СПб: изд. РГГМУ, - 2008, - с. 60.

13. Марчуков А. В. «Беспроводные информационные сети»Учебное пособие. – Томск: изд. Томского политехнического университета, - 2009, - с. 84.

14. Каторин Ю.Ф., Разумовский А. В., Спивак А. И «Защита информации техническими средствами» Учебное пособие под редакцией Каторина Ю. Ф. – СПб: НИУ ИТМО, - 2012, - с. 416.

15. Беспроводные сети WLAN [Электронный ресурс] / Дом Бизнес Строй. — Режим доступа: \www/ URL: https://www.cisco.com/web/RU/products/hw/wireless/pdf/stepstosecurity.pdf / — 04.03.2011 г. — Загл. С экрана

16. Дубовцев В.А. Безопасность жизнедеятельности. / Учеб. пособие для дипломников. - Киров: изд. КирПИ, 1992.

17. Мотузко Ф.Я. Охрана труда. – М.: Высшая школа, 1989. – 336с.

18. Безопасность жизнедеятельности. /Под ред. Н.А. Белова - М.: Знание, 2000 - 364с.

19. Самгин Э.Б. Освещение рабочих мест. – М.: МИРЭА, 1989. – 186с.

20. Справочная книга для проектирования электрического освещения. / Под ред. Г.Б. Кнорринга. – Л.: Энергия, 1976.

21. Борьба с шумом на производстве: Справочник / Е.Я. Юдин, Л.А. Борисов; Под общ. ред. Е.Я. Юдина – М.: Машиностроение, 1985. – 400с., ил.

22. Зинченко В.П. Основы эргономики. – М.: МГУ, 1979. – 179с.

23. Руководство пользователя смартстанции Tellus

24.Татарникова Т.М. Защищенные корпоративные сети. – М. РГГМУ 2012. – 112с.

25. Петраков А.В. Утечка и защита информации в телефонных каналах – М.:Радиософт 2014

26. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации/ М.2009- 280с

Приложение А

Технические характеристики.

– Порты и интерфейсы:

WAN – 1xRJ-45 (10/100/1000 Ethernet)

LAN – 4xRJ-45 (10/100/1000 Ethernet)

WLAN – IEEE 802.11 a/b/g/n (до 300мбит/с)

USB 2.0 – 2 интерфейса

DECT-GAP с CAT-Iq v2.0, подключение 5 DECT трубок

ADSL/ADSL2/ADSL2+ опционально

FXS 2xRJ-11 порта для аналоговых телефонов

FXO 1xRJ-11 порт для внешней телефонной линии

– Построение беспроводной сети Wi-Fi и локальной сети:

IEEE 802.11 a/b/g/n (до 300мбит/с)

Поддержка MultiSSID (до 4 SSID одновременно)

Одновременная работа в двух диапазонах частот 2.4 ГГц и 5 ГГц

Гостевой Wi-Fi доступ

Поддержка WMM (Wi-Fi QoS, 802.11e)

Методы шифрования WEP, WPA и WPA2

Возможность подключить внешние 3G/4G USB-модемы

Приоритизация трафика

– Организация телефонной связи

Подключение до 27 абонентов (SIP телефоны + DECT – телефоны + аналоговые телефоны)

Встроенная DECT база на 5 трубок

Голосовое меню(DISA/IVR)

Получение факса на E-mail

Конференц-связь

Голосовой набор

Заказ вызова из любой точки мира (Web call)

Обратный вызов и множество других функций АТС

– Дополнительные технические данные по телефонии

Протоколы SIP, SDP, RTP

Кодеки G.711 A-law, G.711 law.G729,GSM,G.726,G.722,PCM, DTMF – RFC 2833, SIP INFO, Inband mode

Подавление эха

VAD,CNG,PLC

Джиттер-буфер

Факс – T.38 (RFC 3362)/ G.711 (Pass-through)

– При подключении внешнего USB-диска или принтера:

Функция сетевого хранилища/ поддержка Network access

Storage(NAS)

Встроенный FTP/SMB-Сервер

Принт-сервер

Ограничение доступа к ресурсам NAS для различных пользователей

Приложение Б

Общий вид смарт-станции Tellus