СОДЕРЖАНИЕ

ВВЕДЕНИЕ

По мнению большинства специалистов по информационным технологиям, локальная вычислительная сеть является неотъемлемой частью любого современного общественного здания, а ее отсутствие рассматривается управленческим и техническим персоналом как анахронизм и существенно снижает рыночную стоимость объекта недвижимости.

Проектирование локальной вычислительной сети связано с переносом и размещением на этаже здания автоматизированных рабочих мест, подключенных к локальной вычислительной сети, функция которых сопряжена с хранением и коллективным использованием информации пользователями сети. В данной сети подразумевается возможность печати документов, наличие доступа в Интернет, обеспечение доступа пользователей к базе данных и базе различной руководящей документации (приказам, инструкциям), должна обеспечиваться работа с пакетами прикладных программ. Обеспечение повышенной оперативности оформления документации по различной деятельности цеха и повышения производительности труда персонала в результате более эффективного и экономного использования ресурса компьютеров и информации.

В настоящее время при решении задач защиты конфиденциальной информации в органе государственной власти, на предприятии, в коммерческой организации или в учреждении наиболее значимую роль играют меры организационного характера, способные по своей сути объединить в комплексе все имеющиеся способы и методы защиты информации на основе действующих норм и правил.

Многообразие функций и задач, решаемых предприятиями различных сфер деятельности и организационно-правовых форм, требует постоянного совершенствования системы защиты конфиденциальной информации, принятия новых нормативных актов, методических документов, инструкций и руководств для работников предприятия.

Для решения данной задачи необходимы разносторонние знания нормативно-правовых основ защиты информации, направлений деятельности предприятий, очередности и порядка принятия управленческих решений в зависимости от выбранного комплекса мероприятий.

1 ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ТЕМЫ

1.1 Сетевые топологии

Сетевая топология представляет собой геометрическую форму сети, обозначаемую обычно в виде графа. В зависимости от топологии узловых соединений, существуют такие сети как: кольцевая, шинная, иерархическая, звездная и произвольной структуры.

Кольцевая - узлы этого вида сетей связанны по линии передачи данных, то есть подходят только две линии к каждому из узлов. Когда данные проходят по кольцу, они становятся доступны каждому из узлов, поочередно. Кольцевая топология представлена на Рисунке 1.1.

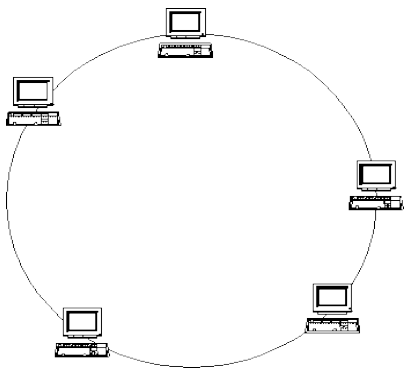

Рисунок 1.1 – Кольцевая топология.

Шинная - топология этого вида сети предполагает, что коммутационный путь служит средой для передачи данных. К этому пути подключены рабочие станции, которые в любой момент времени могут вступить в связь с любой другой станцией сети. Шинная топология показана на Рисунке 1.2.

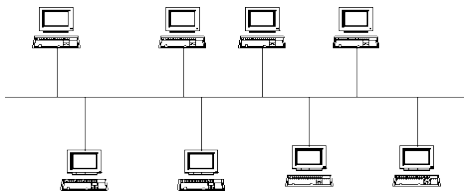

Рисунок 1.2 – Шинная топология.

Звездная – в сети такой топологии существует центральный узел, от которого соединения расходятся ко всем остальным узлам. Такой вид сети представлен на Рисунке 1.3.

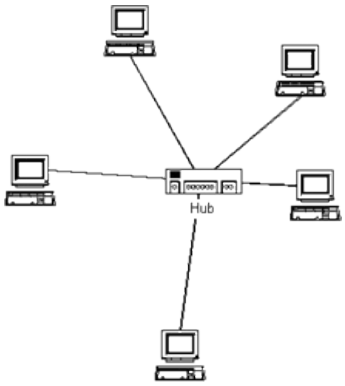

Рисунок 1.3 – Звездная топология.

Иерархическая – сеть такой топологии похожа на звездную расширенную топологию. В такой сети отсутствует центральный узел, вместо него используется магистральный узел, от которого ветви идут к другим узлам. Такая топология, представленная на Рисунке 1.4. Иерархическая топология разделяется на два вида:

– Магистральное дерево – главный магистральный узел имеет ветви-узлы, по которым идут каналы к станциям.

– Бинарное дерево – от каждого из узлов отходит по два соединения.

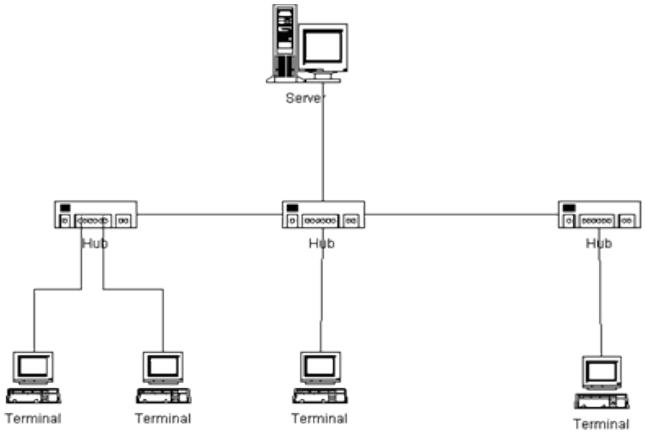

Рисунок 1.4 – Иерархическая топология.

Произвольная структура сети – топология такой сети может получиться исходя из удаления одной или нескольких связей из вышеприведённых видов топологий. Единственным условием такой сети является то, что она должна быть связанной.

2 СРЕДЫ ПЕРЕДАЧИ ДАННЫХ

2.1 Хронология развития структурированных кабельных систем

Вплоть до 1984 годы сооружения проектировались почти в полном отсутствии учета телекоммуникационных сервисов, которые должны были в дальнейшем времени функционировать в них. Появляющиеся программные приложения для передачи данных, поднимали вопрос о использовании специальных типов кабельных систем. Так, например, кабельная система IBM S/3X использовала твинаксиальные кабели в 100 0м, а Ethernet – коаксиальные в 50 0м. В это время все местные существующие телефонные компании могли производить монтаж своих кабельных систем для на стадии проектирования и строительства здания для приложений передачи данных. Специалисты по монтажу систем передачи данных имели доступ на объект уже в то время, как он становился используемым или заселенным.

Инфраструктура подвергалась сложным изменения, зачастую за счет огромных дополнительных затрат средств, и конечно к недовольству конечного пользователя. В данный период речевые (для передачи голоса) кабельные системы не имели развитой структуры. Так, например, обычная кабельная система в бизнес здании существовала из витой пары, которая была неэкранированной (НВП – Unshielded Twisted Pair, UTP), при этом с такими характеристиками, которые могли быть пригодны только для передачи звука или речи, и использовала звездную топологию. Число витых пар, приходящих в ключевые узлы было в диапазоне от 1 до 25.

Более ранние виды кабельных систем, которые использовались для передачи данных в 60-ых годах, имели упор, как правило на передачу несбалансированных сигналов по кабелю типа – «витая пара» между терминалами и хостами-компьютерами. Такой вид кабельной системы мог использоваться только для коммуникации, которые имели низкую скорость, и, со временем, как скорости передачи начали расти, лимитация, связанная с технологией передачи несбалансированных данных по кабелям типа – «витая пара», стала слишком заметной.

После того как появилась технология Ethernet в первой половине 80-ых годов, коаксиальный кабель с сопротивлением в 50 Ом начинает использоваться в коммерческих зданиях. По мере популяризации технологии Ethernet, лидирующие производители оборудования, такие как Bay Networks и Cabletron, начинают производить сетевое интерфейсное оборудование с модульным разъемом за место коаксиального коннектора.

Согласно статистики несовершенные кабельные системы считаются причиной до 75 % всех простоев современной информационной сети. При монтаже СКС, воспроизведенной в соответствии с положениями стандартов, возможно эффективно устранить значительную часть временных простоев.

Невзирая, что кабельная система, как правило, используется дольше большинства других сетевых приложений и компонентов, ее себестоимость составляет совсем небольшую долю общих средств, инвестированных в информационную сеть. То есть, использование структурированной кабельной системы считается достаточно убедительным методом инвестирования в производительность и эффективность любой компании или предприятия.

Кабельная система считается элементом сети с самым длительным временем работоспособности, дольше которого существует только само здание. Кабельная система, используемая на основе стандартов, может гарантировать долговременную функциональность сети и поддержку огромного числа приложений, обеспечив отдачу от инвестирования на всем протяжении её работы.

2.2 Витая пара.

Линия передачи данных, типа – «витая пара» может представлять собой, минимум два проводника, которые разделены диэлектрическими материалами и имеющие равномерные зазоры на всем протяжении передачи. К этим двум проводникам накладывается сбалансированное напряжение, которое равно по амплитуде и противоположно по фазе. Во всех проводниках проходят одинаковые по величине и противоположные по течению токи.

Проходящие токи создают концентрическое магнитное поле, которое окружает каждый из имеющихся проводников. Напряжение магнитного поля всегда увеличивается в отрезке между проводниками и гаснет в пространстве, где концентрическое поле находится за пределом двух проводников. Ток в каждом из проводников равен по величине и противоположен по направлению, это предполагает уменьшение всей энергии, которая собирается в результирующем магнитном поле. Любое изменение силы тока, будет генерировать напряжение на каждом из проводников с результирующим электрическим полем, с направлением течения, которое ограничивает магнитное поле и поддерживает постоянный ток.

Характеристический импеданс – является конечным импедансом любой линии передачи. Такой импеданс равен входному импедансу линии передачи данных, которая однородна и с бесконечной длиной, то есть в идеальном случае линии передачи предельной длины, терминированной (согласованной) нагрузкой с числом ее собственного характеристического импеданса. В итоге, характеристический импеданс – это комплексное значение (число) с реактивной и резистивной компонентами. Он считается функцией частот передаваемых сигналов и не зависит от протяженности линии. При очень высокой частоте характеристический импеданс без сопротивления стремится к определенному резистивному сопротивлению. Например, коаксиальный кабель обладает импедансом величиной 50 или 75 Ом на высокой частоте. Обычное значение импеданса для кабеля типа – «витая пара» это импеданс в 100 Ом при частотах, которые выше 1 МГц.

Сигнал-шум (отношение) – это разница или отношение между уровнем принятия сигнала и уровнем принятия шума, при этом уровень сигналов должен значительно превосходить уровень шумов для обеспечения достаточно приемлемых условий передачи.

Отношение затуханий к переходным затуханиям. Отношение сигнала и шума можно выразить в виде отношения затуханий к переходным затуханиям – ACR. ACR – является разницей между ослабленными сигналами на выходе и вредными наведенными сигналами (шумом). Разрез «витой пары» представлен на Рисунке 2.1.

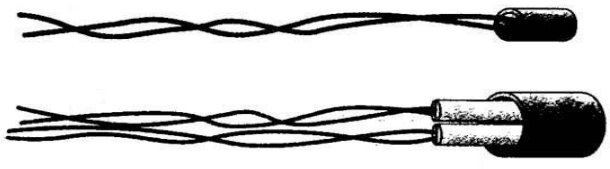

Рисунок 2.1 - Неэкранированная и экранированная витые пары.

2.3 Волоконно-оптический кабель.

Оптические кабельные коммуникации обладают рядом преимуществ перед кабельными системами, которые используют передающую среду на металлической основе. В оптических кабельных системах передаваемый сигнал не искажается ни одним из видов внешних помех – электронных, магнитных и радиочастотных. То есть, на оптические кабельные сети полностью исключается воздействие помех, вызываемым молниями или источниками высокого напряжения. Кроме того, оптические волокна не испускают излучений, что возводит его в ряд идеальных, для соответствия требованию современного стандарта к компьютерным приложениям.

Исходя из того, что оптический сигнал не требует наличия системы заземления, получается, что передатчик и приемник изолированы (диэлекртизованны) друг от друга, а также отсутствуют проблемы, связанные с возникновением паразитной токовой петли. При отсутствии или недостатке сдвига потенциала в системе заземления между двух терминалов, которые исключают искрения и различные электрические разряды, волоконная-оптическая.

Размер оптических волокон для обеспечения нормальной работоспособности определяется по внешнему диаметру ядра, характеристикам демпфера и оболочки. Например, 50/125/200 – характеристика оптического волокна с диаметром ядра в 50 мкм, диаметром демпфера 125 мкм и диаметром оболочки 200 мкм. Оболочка всегда убирается при соединении волокон.

Вид волокна определяется по типу пути, или так именуемых «мод», которые проходят светом в ядре волокна. Существуют два основных вида оптического волокна: многомодовое и одномодовое. Ядро многомодового волокна может обладать ступенчатыми или градиентными показателями преломления.

Многомодовое оптическое волокно со ступенчатыми показателями преломления обрело свое название от внезапной, ступенчатой, разницы среди показателей преломления ядер и демпфера. В более популярном многомодовом оптическом волокне с градиентными показателями преломления, луч света разносится в волокне по многим путям. В отличие от оптического волокна со ступенчатыми показателями преломления, ядра с градиентными показателями содержат большое количество слоев стекла, которые обладают наиболее меньшим показателем преломления по сравнению с предшествующим слоем по мере удаления от центра волокна.

Итогом формирования таких градиентов показателей преломления является то, что луч света ускоряется в верхних слоях и время распространения в оптических волокнах соизмеряется с временем распространения луча, проходящего по наиболее мелким путям, ближе к центру волокна. Градиентное многомодовое волокно представлено на Рисунке 2.2.

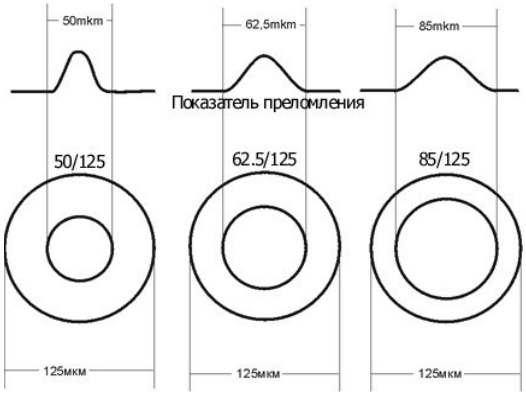

Рисунок 2.2 - Градиентное многомодовое волокно.

Исходя из этого, волокна с градиентными показателями преломления выравнивают время распространения всевозможных мод так, что передающиеся данные по волокну, могут передаваться на значительно большие расстояния и на значительно более больших скоростях до того времени, пока импульсы света не начнут сливаться и становиться неразличимыми на стороне приема. Ступенчатое многомодовое волокно показано на Рисунке 2.3.

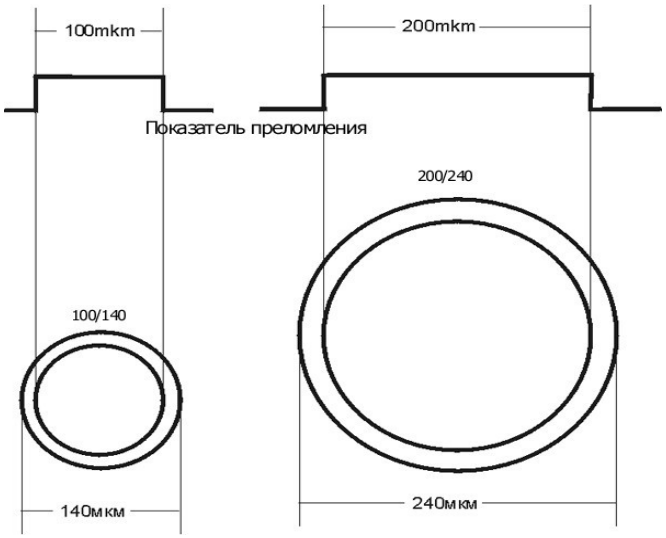

Рисунок 2.3 – Ступенчатое многомодовое волокно.

Одномодовые оптические волокна, в отличие от многомодовых, позволяют распространяться только лишь одному из лучей или моде света в ядрах. Это исключает любое искажение, которое вызывается перекрытием импульсов. Диаметры ядер одномодовых волокон чрезвычайно малы – примерно 5–10 мкм.

Одномодовые волокна обладают наиболее высокими пропускными способностями, чем любые из многомодовых видов. Например, использующиеся под водой оптоволоконные кабели могут нести 70000 речевых каналов по одной из пар одномодового волокна.

Ступенчатое одномодовое волокно представлено на Рисунке 2.4.

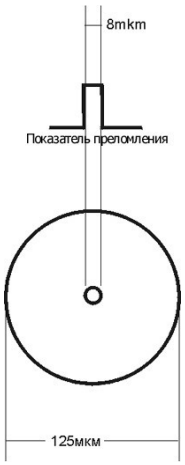

Рисунок 2.4 – Ступенчатое одномодовое волокно.

2.4 Коаксиальный кабель.

Так же, как и витая пара, коаксиальный кабель состоит из двух медных проводников, только эти проводники расположены не параллельно, а концентрически (или коаксиально). С помощью такой конструкции, а также благодаря специальной изоляции и экранирования, коаксиальный кабель позволяет достичь высоких скоростей передачи данных. Он часто используется в системах кабельного телевидения. Системы кабельного телевидения в сочетании с кабельными модемами могут обеспечивать для абонентов доступ в Интернет на скоростях в десятки мегабит в секунду. В кабельном телевидении, а также в кабельных сетях доступа передатчик переносит цифровой сигнал в определенную полосу частот, и затем результирующий аналоговый сигнал посылается от передатчика к одному или нескольким приемникам.

Коаксиальный кабель может использоваться как разделяемая проводная среда. К кабелю могут быть непосредственно подключены несколько конечных систем, и каждая из них может принимать данные.

Вид коаксиального кабеля в разрезе представлен на Рисунке 1.2.5.

Рисунок 2.5 – Коаксиальный кабель.

3 СТАНДАРТЫ ПЕРЕДАЧИ ДАННЫХ

3.1 Сетевая технология IEEE802.3 Ethernet.

Существует множество разновидностей Ethernet, которые обозначаются довольно сложными аббревиатурами, например, 10BASE-T, 10BASE-2, 100BASE- T, 1000BASE-LX и 10GBASE-T. Эти и многие другие технологии Ethernet были стандартизированы за прошедшие годы рабочей группой IEEE 802.3 CSMA/CD (Ethernet). Сокращения на первый взгляд могут показаться устрашающими, но на самом деле в них прослеживается определенный порядок. Первая часть аббревиатуры указывает на скорость, применяемую в стандарте: 10, 100, 1000 или 10G означает, соответственно, 10 Мбит/с, 100 Мбит/с, 1 Гбит/с и 10 Гбит/с. BASE означает немодулированный Ethernet – то есть физический носитель передает только трафик Ethernet; практически все стандарты 802.3 касаются именно немодулированного Ethernet. Последняя часть аббревиатуры описывает сам физический носитель.

Для Ethernet существуют спецификации как канального, так и физического уровня, а передача данных осуществляется по разнообразным физическим носителям, включая коаксиальный кабель, медный кабель и оптоволокно. Вообще буква T означает медный кабель типа «витая пара».

Исторически технология Ethernet задумывалась для передачи информации по коаксиальному кабелю. Ранние стандарты 10BASE-2 и 10BASE-5 описывают Ethernet-передачу со скоростью 10 Мбит/с по 2 типам коаксиального кабеля, в обоих случаях длина кабеля не должна превышать 500 м. Передача на более длинные дистанции осуществляется при помощи повторителя. Это устройство физического уровня, которое принимает на входе сигнал и воспроизводит его на выходе. Все кадры, передаваемые интерфейсом, принимаются на всех остальных интерфейсах, а протокол Ethernet CDMA/CD хорошо решает проблему множестве.

В середине 90-х появился стандарт Ethernet со скоростью передачи данных 100 Мбит/с – то есть в 10 раз быстрее, чем 10 Мбит/с. В нем сохранились оригинальный протокол Ethernet MAC и формат кадра, но были описаны более высокоскоростные физические уровни для медного кабеля (100BASE-T) и для оптоволоконного кабеля (100BASE-FX, 100BASE-SX, 100BASE-BX). На Рисунке 3.1 представлены эти различные стандарты, а также обычный протокол Ethernet MAC и формат кадра.

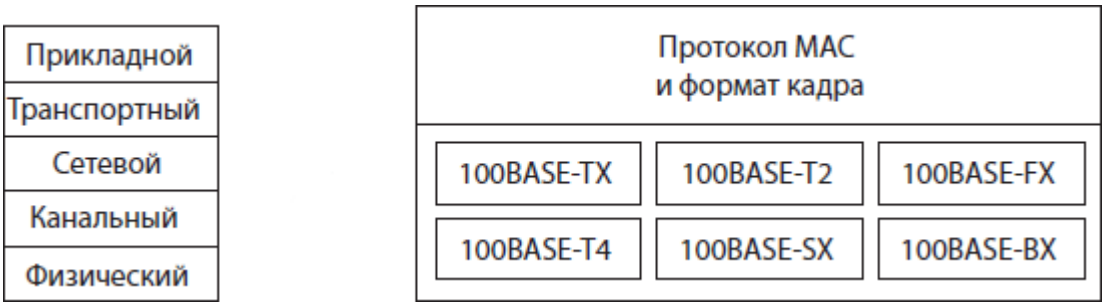

Рисунок 3.1 - Стандарты Ethernet 100 Мбит/с.

3.2 Стандарты технологии Wi-Fi.

Прочно обосновавшиеся на рабочих местах, в наших домах, образовательных учреждениях, кафе, аэропортах и уличных перекрестках, беспроводные локальные сети превратились в одну из самых важных технологий доступа к Интернету.

Несмотря на то, что в 1990-х годах велись разработки большого количества технологий и стандартов для беспроводных локальных сетей, победителем этого состязания стал лишь один класс стандартов беспроводных сетей: беспроводная локальная сеть IEEE 802.11 wireless LAN, или просто Wi-Fi.

Существует несколько стандартов беспроводных локальных сетей 802.11, в том числе 802.11b, 802.11a и 802.11g. В Таблице 3.1 приводится краткое обобщение характеристик вышеперечисленных стандартов, впрочем, стандарт 802.11g по популярности далеко опережает своих собратьев. Кроме того, сегодня доступны устройства, работающие в двойном (802.11a/g) и даже тройном (802.11a/b/g) режимах.

Между всеми тремя стандартами семейства 802.11 есть очень много общего. Так, например, они используют одинаковый протокол доступа к среде передачи данных, CSMA/CA. Структуры кадров канального уровня всех трех стандартов также идентичны. Все три стандарта обладают возможностью уменьшать скорость передачи данных с целью достижения более дальних расстояний.

Таблица 3.1 - Характеристики семейства стандартов IEEE 802.11.

Стандарт	Диапазон частот (Россия) Мгц.	Скорость передачи данных Мбит/с
802.11b	2400 - 2483,5	до 11
802.11a	5150 - 5350	до 54
802.11g	2400 - 2483,5	до 54

4 СРАВНЕНИЕ ОТЕЧЕСТВЕННЫХ И ПЕРЕДОВЫХ ЗАРУБЕЖНЫХ ТЕХНОЛОГИЙ И РЕШЕНИЙ.

4.1 Развитие технологии Ethernet.

Предполагается следующий рост потребности в пропускной способности трафика в сетях Ethernet: в ближайшее время понадобится скорость в 1 Тбит/с, а к 2020 г. – 10 Тбит/с. В наибольшей степени скорости повысятся в центрах обработки данных, трафик в них растет не только между серверами и распределенными клиентами, но и между оборудованием внутри центра, что связано с обеспечением функционирования виртуализированных сред и «облаков».

IEEE изучил перспективы реализации систем со скоростью более 100 Гбит/с, решено увеличить скорость в четыре раза – до 400 Гбит/с, т.е. необходима разработка технологии 400GbE. В стандарте IEEE 802.3ba поддерживаются две скорости: 40 и 100 Гбит/с. Эти скорости обеспечивают совместимость с оптическими транспортными системами дальней связи OTN.

Поток в 400 Гбит/с можно получить различными способами. Обсуждаются варианты: 16 потоков по 25 Гбит/с, 8 по 50 Гбит/с, 4 по 100 Гбит/с.

Наиболее вероятной реализацией 400GbE в ближайшее время может быть вариант с 16 электрическими потоками, которые преобразуются в конверторе в световые потоки, и далее подаются в мультиплексор спектрального уплотнения, который выдает 16 составляющих в одно MUX одномодовое волокно.

Реализация такого потока представлена на Рисунке 4.1

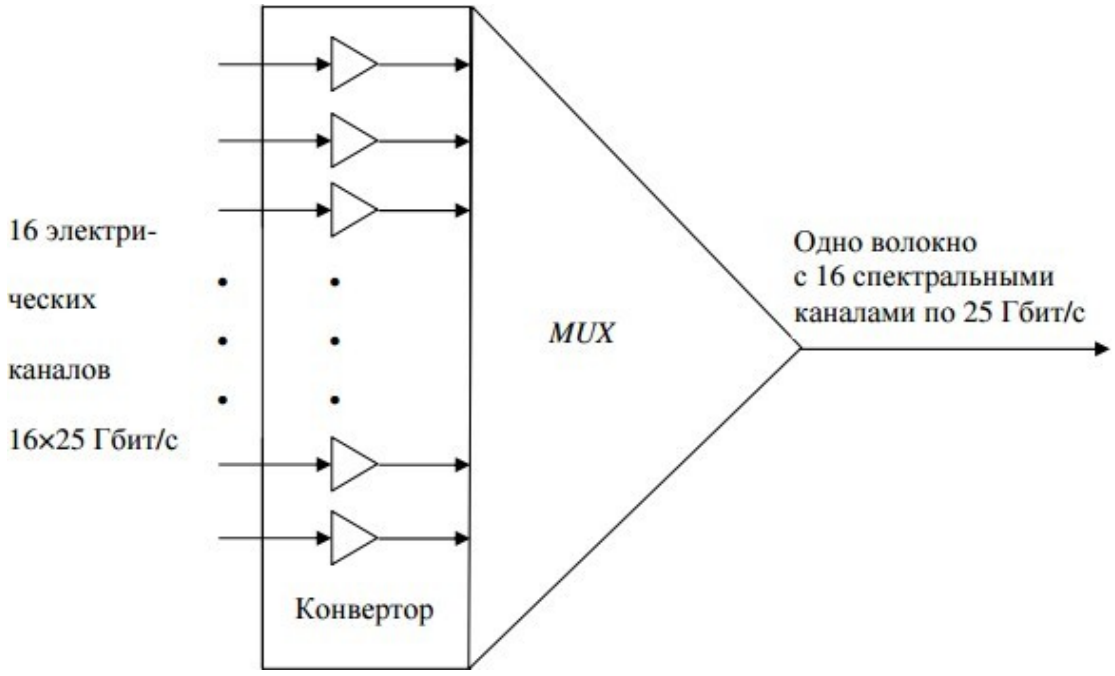

Рисунок 4.1 – Реализация потока в 400 Гбит/с.

4.2 Технология Infini Band.

Infini Band является высокоскоростной коммутируемой компьютерной сетью, которая используется для высокопроизводительных вычислений, имеет очень большую пропускную способность и низкие задержки. Кроме того, может использоваться для внутреннего соединения в некоторых вычислительных комплексах. По состоянию на 2017 год Infini Band является самой популярной сетью для суперкомпьютеров.

В области компьютерных технологий сформировалось новое направление: «вычисления на лезвиях» (Blade Based Computing, BBC). Центр обработки данных формируется из необходимого пользователя коммуникационных и вычислительных компонентов. В основе BBC лежит концепция архитектуры Infini Band, обеспечивающая разделение доступа к ресурсам.

С началом производства ультратонких серверов («серверных лезвий», server blade) толщиной 1U и 2U (1U = 1,75 дюйма) появилась возможность создания стоек из «серверных лезвий» (Blade Frame). В одну стойку устанавливается десятки материнских плат. Каждая плата (модуль) включает процессор, оперативную память, сетевые интерфейсы и служебные схемы. Все модули имеют общую внешнюю (дисковую) память, общую систему энергообеспечения и охлаждения.

Системы на основе «серверных лезвий» могут использоваться в следующих вариантах:

- сетевой хост (Web-сервер) глобальной сети (сервер может объединять несколько сот независимых серверов);
- высокопроизводительная вычислительная система;
- процессорная сеть и сеть хранения информации.

Процессорная сеть (PAN, processing area network) объединяет двух, четырех процессорных лезвия. В состав PAN входят интегральные коммутаторы, контроллеры и шины для объединения в кластеры. Сеть имеет единую точку управления. Сети PAN являются развитием концепции сетей хранения (SAN, storage area network). Сеть хранения информации представляет собой быстродействующую отказоустойчивую

информационную систему.

PAN и SAN, собранные в одной стойке, могут образовывать готовую инфраструктуру для операторов информационных услуг или для пользователей корпоративной информационной системы. Таким образом, стойка с лезвиями может использоваться как сервер, как сеть и как система хранения.

В стойках с лезвиями используются «серверы-лезвия» трех типов как показано на Рисунке 4.2.

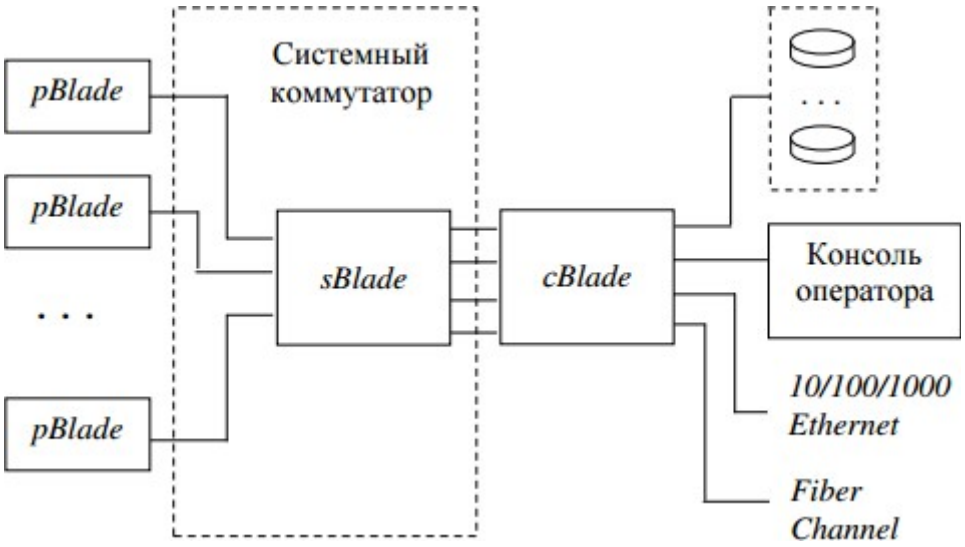

Рисунок 4.2 – Использование «серверов-лезвий».

Процессорные «лезвия» (Processing Blade, pBlade) содержат дублированные процессоры и оперативную память. Процессорные лезвия не имеют внешних запоминающих устройств, то есть их конфигурация унифицирована, и поэтому они полностью взаимозаменяемы.

- Коммутирующие «лезвия» (Switch Blade, sBlade) соединяют серверы pBlade с панелью стойки Blade Plane. Панель служит интерфейсом. Серверы sBlade имеют 4 процессора, полностью резервированы, управляют внешним и внутренним трафиком.

- Управляющие «лезвия» (Control Blade, cBlade) полностью резервированы. На cBlade размещается ПО управления процессорной сетью. На этих модулях размещаются сетевые порты (витая пара 10/100/1000 Ethernet, Fiber Channel), а также порт для подключения консоли оператора. cBlade обеспечивает интерфейс с внешней памятью.

В стойке различные модули объединяются посредством шин панели стойки Blade Plane. Имеются основная и резервная шины. Совместно с модулями sBlade шины образуют системный коммутатор (внутреннюю сеть TCP/IP). Системный коммутатор можно считать виртуальным, так как конфигурация может изменяться. Скорость коммутации – примерно 200 Мбайт/с. В составе ОС имеется менеджер сети (PAN Manager), выполняющий функции:

- определение конфигурации системы;
- образование виртуальных серверов из пула лезвий;
- увязывание виртуальных серверов с дисковыми и сетевыми ресурсами;
- создание динамических кластеров из виртуальных серверов.

В системе с серверными лезвиями всё задублировано (коммутация, питание, охлаждение и др.), в том числе часы. В каждом модуле имеются свои часы. Таким образом, не существует единой точки выхода сети из строя.

Использование технологии Infini Band для внутрисетевых взаимодействий дает следующие преимущества перед другими подобными технологиями:

- более высокий уровень качества Qos (качество обслуживания), учитывающий контроль прохождения данных и существующую систему приоритетов; большая гибкость, позволяющая строить кластеры;
- лучшие значения показателей RAS (службы удаленного доступа); осуществляются циклические проверки, проводится контроль соединений, возможны альтернативные маршруты; в целом сеть Infini Band способна к восстановлению.

5 ПРОЕКТИРОВАНИЕ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ.

5.1 План проектирования сети.

Проектирование локальной вычислительной сети цеха промышленного водоснабжения связано с переносом и размещением на этаже здания автоматизированных рабочих мест (АРМ), подключенных к локальной вычислительной сети, функция которых сопряжена с хранением и коллективным использованием информации пользователями сети.

В данной сети подразумевается возможность печати документов, наличие доступа в Интернет, обеспечение доступа пользователей к базе данных и базе различной руководящей документации (приказам, инструкциям), должна обеспечиваться работа с пакетами прикладных программ.

Кроме того, ЛВС должна обеспечивать повышение оперативности оформления документации по различной деятельности цеха и повышения производительности труда персонала в результате более эффективного и экономного использования ресурса компьютеров и информационного обеспечения.

Для проектирования ЛВС подразделения необходимо:

- Прокладка волоконно-оптической лини связи между зданием, в котором располагаются сервера и зданием куда переезжает подразделение.
- Установка напольного шкафа на 19 дюймов в здании организации кабельной сети.
- Установка в шкафу оптических полок и подвод оптического кабеля.
- Размещение автоматизированных рабочих мест в здании переезда (в соответствии с правилами структурированной кабельной системы).

5.2 Исходные данные.

Локальная вычислительная сеть подразделения должна разместиться в 3- этажном здании офисного значения, у других этажей которого имеется идентичная планировка, представленная на Рисунке 5.1 на примере этажа на котором будет размещена кабельная система. Общая высота этажа здания между перекрытиями равна 3 метрам, общая толщина междуэтажных перекрытий здания равна 40 см, а толщина стен составляет 15 см.

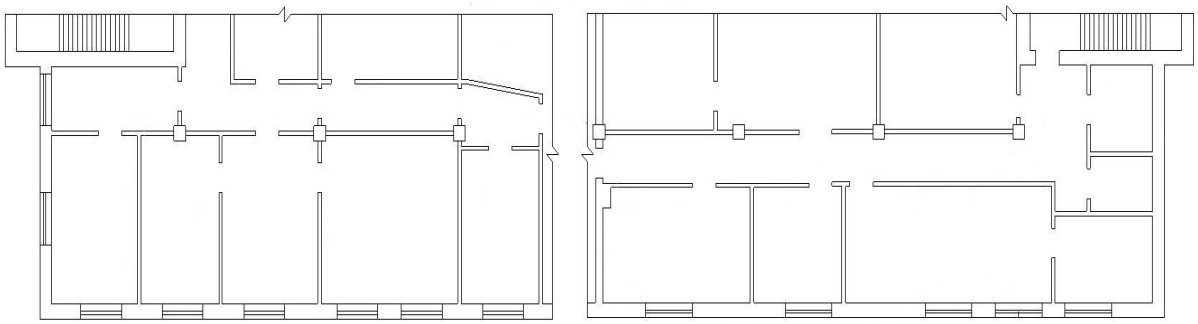

Рисунок 5.1 – План этажа, предназначенного для переноса АРМ.

На стенах этажа имеется довольно много свободного места для расположения лотков, которые предназначены для прокладки кабелей различного назначения. Стены этажа и внутренние перегородки, которые отделяют помещения друг от друга, сделаны из обычного кирпича, с нанесенным на него слоем штукатурки, толщина которой равна 1 см. Каких-либо других дополнительных каналов на полах и стенах этажа, которые могут использоваться для прокладки кабеля, не предусмотрено строительным проектом здания.

Кабельные входы в технологические помещения и помещения офисного типа для пользователей должны быть смонтированы в виде асбестоцементных труб.

6 АРХИТЕКТУРНАЯ ФАЗА ПРОЕКТИРОВАНИЯ.

6.1 Монтаж телекоммуникационных розеток.

Этаж здания, на котором будет произведено перемещение кабельной системы согласно плану, имеет по 10 рабочих мест в помещениях, которые предназначаются для размещения пользователей. Размещение рабочих мест представлено в приложении А.

В соответствии с государственным стандартом ГОСТ Р 53246-2008 коннекторы устанавливаемых телекоммуникационных розеток должны обладать надежным креплением на рабочих местах.

Расположение розетки на рабочем месте должно быть определено

так, чтобы обеспечивалось подключение активного оборудования при помощи аппаратных шнуров длиной не больше 5 м.

Рекомендовано производить монтаж розетки на рабочем месте рядом с электрическими розетками (желательно в пределе 1 м) и с идентичной высотой.

При монтаже розеток пристальное внимание уделяется их расположению относительно мебели помещения, так как различные шнуры, которые подключаются к розеткам и проходят через открытые места полов, представляют потенциальную опасность для пользователя.

Диапазон температуры в месте монтажа розеток должен иметь диапазон от - 10°С до +60 °С.

Коммутационная аппаратура должна обладать защитой от механических повреждений, влияний повышенного уровня влажности и других коррозирующих факторов.

6.2 Правила монтажа кабелей.

Рабочие характеристики кабелей и коммутационной аппаратуры могут существенно меняться вследствие нарушений правил монтажа и последующей манипуляции с кабельными потоками. Монтаж и обслуживание фиксированного кабельного сегмента горизонтальных и магистральных подсистем отличается от правил организации коммутационного кабеля в кроссах. Кроссированное соединение предназначено для обеспечения гибкости проведений изменений в схеме коммутаций.

К мере предосторожности, соблюдаемой при монтаже и развертывании кабельного потока, относится исключение различного

вида механических напряжений на кабеле, которые вызываются натяжением, резким изгибом и чрезмерными стягиваниями пучков кабеля. При монтаже кабеля в трассах и телекоммуникационном помещении следует пользоваться средствами маршрутизации кабельного потока, их крепления и фиксирования.

Кабельный хомут (стяжка, бандаж и т. п.), которые используются для организации кабельного пучка, должны располагаться на пучках так, чтобы хомуты могли свободно перемещаться в продольных и поперечных направлениях. Нельзя допускать затягивания хомутов, приводящего к деформации оболочки кабеля.

Нельзя допускать крепление телекоммуникационного кабеля с помощью скоб. Кроме того, нельзя допускать использования лифтовой шахты для монтажа кабеля на основе любых разрешенных типов среды передачи. Нужда в сохранении минимальных радиусов изгиба кабелей на основе «витой пары» проводника обусловлена тем, что при резком изгибе пары внутри кабелей искажается и нарушается однородность симметричных сред передачи.

Это представляется, в первую очередь, серьезными изменениями такого параметра, как NEXT (переходное затухание). Последующие распрямления изгибов могут не только не вернуть форму пары, но и привести к еще более худшему результату.

Согласно ГОСТ Р 53246-2008 радиус изгибов кабеля горизонтальных и магистральных подсистем не должен быть менее:

- Четыре внешних диаметра кабеля для 4-парного кабеля с

неэкранированной витой парой проводника (UTP) в состоянии использования.

- Восемь внешних диаметра кабеля для 4-парного кабеля с неэкранированной витой парой проводника (UTP) в состоянии монтажа.

- 25 мм для оптической кабельной системы внутреннего применения с числом волокон 2 и 4 при использовании кабеля.

- 50 мм для оптической кабельной системы внутреннего применения с числом волокон 2 и 4 при монтаже кабеля.

При монтаже кабеля и в некоторых случаях в процессах его эксплуатации на него действует сила натяжения, способная привести к деформации пар в кабеле в основе которого лежит «витая пара» и механическим повреждения волокон в волоконно-оптическом кабеле. Поэтому одним из главных требований, которые предъявляются к монтажу, это соблюдение предельных допустимых сил натяжения кабелей.

Сила натяжения кабеля горизонтальных и магистральных подсистем в процессе монтажа и эксплуатации не должна превышать:

- 110 Н – для 4-парного кабеля, в основе которого неэкранированная и экранированная витая пара;

- 220 Н или рекомендации производителей в случаях, если он более жесткий для волоконно-оптического кабеля внутреннего использования с числом волокон 2 и 4;

- 2700 Н или рекомендации производителей в случаях, если он более жесткий для волоконно-оптического кабеля внешнего использования.

При монтаже кабельных систем рекомендовано предусматривать запас кабелей на двух концах кабельного сегмента с целью обеспечения возможностей внесения изменения в будущем.

- Рекомендовано оставить следующие запасы кабелей для рабочих мест: кабель в основе которого «витая пара» – 0,3 м;
- волоконно-оптические кабеля – 1 м.

Кабель должен быть терминирован на коммутационном оборудовании с эквивалентными или более высокими категориями рабочих характеристик. Категория рабочей характеристики кабеля и коннекторов определена таким образом, что их влияние на рабочую характеристику линии были незначительными.

С целью сохранения геометрической формы кабеля, в основе которого «витая пара» проводников, при терминировании на коммутационной аппаратуре нужно удалить оболочку настолько, сколько нужно для осуществления данной операции.

Рекомендовано удалить оболочку 4-парного кабеля от точки терминирования проводника не более 75 мм. При терминировании кабеля в основе которого «витая пара» повив пары должен сохраняться вплоть до точек терминирования. Расстояния от точек терминирования до ближайших узлов повива пары должны составлять не более:

- 13 мм – для кабеля с рабочей характеристикой категорий 5е и 6;
- 25 мм – кабеля с рабочей характеристикой категории 3.

6.3 Телекоммуникационная фаза проектирования.

Телекоммуникационная фаза проекта представляет собой разработку конкретной структуры ЛВС, составление перечня необходимого оборудования и планов его размещения.

Главным фактором этой фазы, который определяет количество отдельных компонентов ЛВС, является размер помещений для размещения автоматизированных рабочих мест и конфигурация информационных розеток.

На время проведения проектной работы основным стандартом организации ЛВС считается Ethernet в различных его вариантах. Применение для организации горизонтальных подсистем элементной базы категории 5е обеспечит передачу по тракту кабельной системы сигналов всех обширно распространенных на практике видов этого сетевого интерфейса локальной вычислительной сети, даже с использованием его сверхвысокоскоростных вариантов, например – Gigabit Ethernet 802.3aЬ.

Следовательно, представленное решение обеспечит резерв пропускных способностей горизонтального тракта кабельной системы, достаточного для поддерживания функциональности всего вида перспективных приложений известных на момент проектирования, то есть надежную защиту инвестиций предприятия, сделанных им в кабельной системе цеха.

Проектируемая кабельная система подразделения может быть использована для передачи конфиденциальной информации. Для этого структурированная кабельная система будет строится на более защищенной экранированной элементной базе.

7 ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

7.1 Основные принципы и условия организационной защиты информации.

Организационная защита информации по своей сути является организационным началом, так называемым "ядром" в общей системе защиты конфиденциальной информации предприятия. От полноты и качества решения руководством предприятия организационных задач зависит эффективность решения проблем в данной области в целом.

Роль и место организационной защиты информации в общей системе мер, направленных на защиту конфиденциальной информации предприятия, определяются исходя из исключительной важности принятия руководством правильного и своевременного управленческого решения на основе действующего нормативно-методического аппарата, а также имеющихся в его распоряжении сил, средств, методов и способов защиты информации. Основные направления защиты информации представлены на Рисунке 7.1.

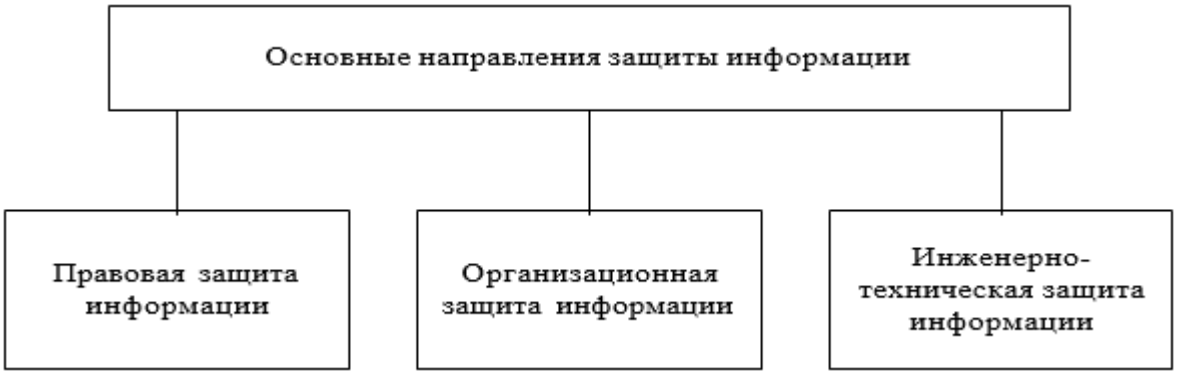

Рисунок 7.1 – Основные направления защиты информации.

Организационная защита информации - составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Организационно-правовая защита информации - регламентация производственной деятельности и взаимоотношений субъектов (сотрудников

предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

Первое из приведенных определений в большей степени показывает сущность организационной защиты информации. Второе - раскрывает ее структуру на уровне предприятия.

Вместе с тем, оба определения подчеркивают важность нормативно-правового регулирования вопросов защиты информации наряду с комплексным подходом к использованию в этих целях имеющихся сил и средств.

Основные направления организационной защиты информации приведены на Рисунке 7.2.

Рисунок 7.2 – Основные направления организационной защиты информации.

Таким образом, организационная защита информации сегодня является важнейшим элементом в общей системе защиты информации предприятия, с высокой эффективностью обеспечивающим ее защиту при условии соблюдения должностными лицами предприятия норм и правил защиты информации, определенных в соответствующих нормативно-методических документах.

Основными принципами организационной защиты информации являются следующие принципы: принцип комплексного подхода к решению задач защиты информации; принцип оперативности принятия управленческих решений; принцип персональной ответственности.

Принцип комплексного подхода заключается в использовании сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу возможной утечки конфиденциальной информации.

Принцип оперативности принятия управленческих решений существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает целеустремленность должностных лиц на решение задач защиты информации.

Принцип персональной ответственности заключается в наиболее эффективном и полном распределении сил структурных подразделений предприятия, участвующих в процессе защиты информации.

Среди основных условий организационной защиты информации можно выделить следующие:

- непрерывность всестороннего анализа состояния системы защиты информации с целью принятия своевременных мер по повышению ее эффективности;
- неукоснительное соблюдение должностными лицами и сотрудниками структурных подразделений предприятия установленных норм и правил защиты конфиденциальной информации.

При соблюдении вышеперечисленных условий будет обеспечено наиболее полное и качественное решение задач по защите конфиденциальной информации на предприятии.

7.2 Основные подходы и требования к организации системы защиты информации.

Успешное решение комплекса задач по защите конфиденциальной информации не может быть достигнуто без создания единой основы, так называемого "активного кулака" предприятия, способного концентрировать все усилия, имеющиеся ресурсы для исключения утечки конфиденциальной информации и недопущения возможности нанесения ему ущерба.

Таким "кулаком" призвана стать система защиты информации на предприятии, создаваемая на нормативно-методической основе в данной области и отражающая все направления и специфику его деятельности.

Под системой защиты информации понимается совокупность органов защиты информации (структурных подразделений или должностных лиц предприятия), используемых ими средств и методов защиты информации, а также мероприятий, планируемых и проводимых в этих целях. Структура системы защиты информации приведена на Рисунке 7.3.

Для решения организационных задач по созданию и функционирования системы защиты информации используются несколько основных подходов, которые вырабатываются на основе существующей нормативно-правовой базы и с учетом методических разработок по тем или иным направлениям защиты конфиденциальной информации.

Один из основных подходов к созданию системы защиты информации заключается во всестороннем анализе состояния защищенности информационных ресурсов предприятия с учетом устремленности конкурирующих организаций к овладению конфиденциальной информацией и, тем самым, нанесению ущерба предприятию.

Важным элементом анализа является работа по определению перечня защищаемых информационных ресурсов с учетом особенностей их

расположения (размещения) и доступа к ним различных категорий сотрудников (работников других предприятий).

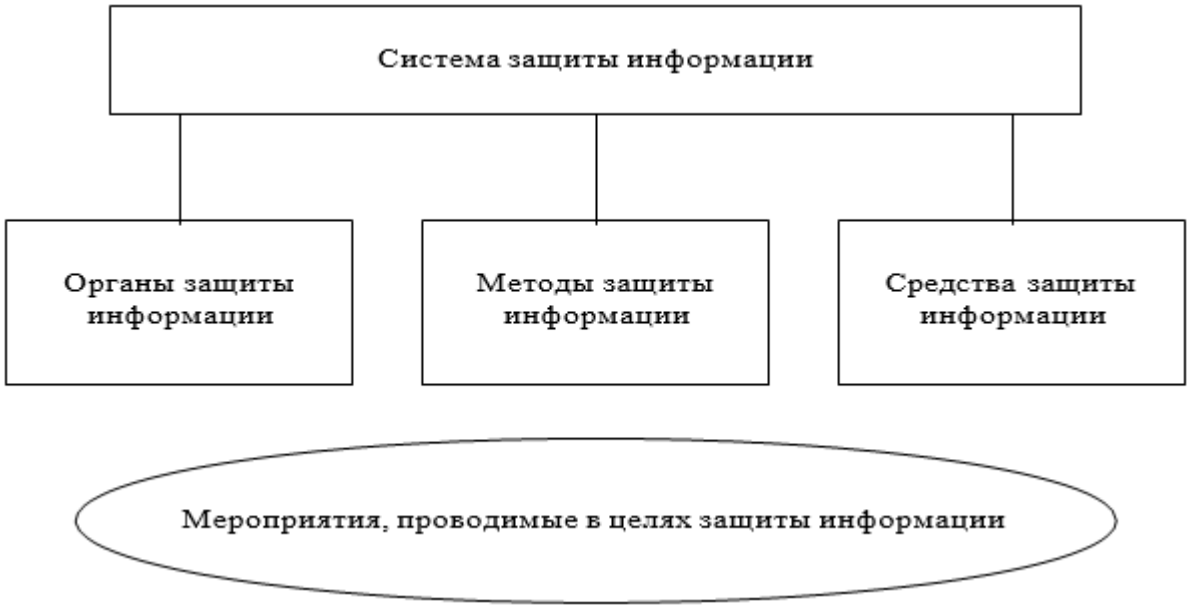

Рисунок 7.3 – Структура системы защиты информации.

Работу по проведению такого анализа непосредственно возглавляет руководитель предприятия и его заместители по направлениям деятельности. Изучение защищенности информационных ресурсов основывается на положительном и отрицательном опыте работы предприятия, накопленном в течение последних нескольких лет, а также наработанных деловых связях и контактах предприятия с организациями, осуществляющими аналогичные виды деятельности.

При создании системы защиты информации, в первую очередь, учитываются наиболее важные, приоритетные направления деятельности предприятия, требующие особого внимания. Предпочтение также отдается новым, перспективным направлениям деятельности предприятия, связанным с научными исследованиями, новейшими технологиями, формирующими интеллектуальную собственность, а также развивающимся международным связям. На этой основе формируется перечень возможных угроз информации,

подлежащей защите, и определяются предполагаемые к использованию в этих целях конкретные силы, средства, способы и методы ее защиты.

К организации системы защиты информации с позиции системного подхода выдвигается ряд требований, определяющих ее целостность, стройность и эффективность. Система защиты информации должна отвечать совокупности следующих основных требований, то есть быть:

- централизованной - соответствующей эффективному процессу управления системой со стороны руководителя и ответственных должностных лиц по направлениям деятельности предприятия.
- плановой - объединяющей усилия различных должностных лиц и структурных подразделений при их участии в организации и обеспечении выполнения задач, стоящих перед предприятием.
- конкретной и целенаправленной - защите должны подлежать абсолютно конкретные информационные ресурсы, представляющие интерес для конкурирующих организаций.
- активной - обеспечивать защиту информации с достаточной степенью настойчивости и возможностью концентрации усилий на наиболее важных направлениях деятельности предприятия.
- надежной и универсальной - охватывать весь комплекс деятельности предприятия, связанной с созданием и обменом информацией.

7.3 Основные силы и средства, используемые для организации защиты информации.

Одним из важнейших факторов, оказывающих существенное влияние на эффективность системы защиты конфиденциальной информации, является совокупность сил и средств предприятия, используемых для организации защиты информации и непосредственно участвующих в этом процессе.

Силы и средства различных предприятий отличаются по структуре, характеру и порядку использования.

Предприятия, осуществляющие работу с конфиденциальной информацией и решающие задачи по ее защите на постоянной основе, то есть в каждодневной деятельности, вынуждены с этой целью создавать самостоятельные структурные подразделения и использовать высокоэффективные средства защиты информации.

Предприятиями, осуществляющими эпизодическую работу с конфиденциальной информацией, в силу ее небольших объемов, вместо создания вышеупомянутых подразделений в штаты своих предприятий могут включаться самостоятельные должности специалистов по защите информации.

Наряду с этим, данные предприятия на договорной основе могут использовать потенциал более крупных предприятий, имеющих необходимое количество квалифицированных сотрудников и высокоэффективные средства защиты информации. Эти вопросы регулируются нормативными актами, определяющими порядок оказания услуг в данной области. Ведущую роль в организации защиты информации на предприятии играет руководитель предприятия, а также его заместитель, непосредственно возглавляющий эту работу.

Руководитель предприятия в соответствии с законодательством несет персональную ответственность за организацию и осуществление необходимых мероприятий, направленных на исключение утечки сведений, отнесенных к конфиденциальной информации, и утрат носителей информации.

Руководитель предприятия при организации работ по защите информации обязан:

- знать фактическое состояние дел по этим вопросам, организовывать постоянную работу по выявлению и закрытию возможных каналов утечки конфиденциальной информации;
- определять обязанности и задачи должностным лицам и структурным подразделениям предприятия в этой области;
- предъявлять высокую требовательность к сотрудникам предприятия в вопросах сохранности сведений конфиденциального характера;
- оценивать деятельность должностных лиц по защите информации и эффективность проводимых в целях защиты соответствующих сведений мероприятий.

Заместитель руководителя предприятия обязан постоянно изучать все стороны и направления деятельности предприятия с целью принятия своевременных мер по защите информации; руководить работой службы безопасности (структурных подразделений по защите государственной тайны), а также выполнять другие функции по организации защиты информации в ходе проведения предприятием всех видов работ.

В структуре предприятий с целью организации работ по защите информации могут создаваться следующие основные виды структурных подразделений:

- режимно-секретные;
- подразделения по противодействию иностранным техническим разведкам и технической защите информации;
- подразделения криптографической защиты информации;
- мобилизационные;

- подразделения охраны и пропускного режима.

Функции, возлагаемые на вышеперечисленные подразделения, определяются решением (приказом) руководителя предприятия и отражаются в соответствующих положениях. Более подробно указанные функции, а также задачи, решаемые данными подразделениями, будут рассмотрены в последующих разделах учебного пособия.

По решению руководителя предприятия вышеупомянутые подразделения могут быть структурно объединены в службу режима предприятия, руководитель которой наделяется статусом заместителя руководителя предприятия, и полномочиями должностного лица, имеющего право осуществлять непосредственное руководство деятельностью всех подразделений предприятия, если их деятельность связана с использованием информации, отнесенной к конфиденциальной информации (государственной тайне) и подлежащей защите.

Характерной особенностью функционирования режимно-секретного подразделения, мобилизационного подразделения и подразделения по противодействию иностранным техническим разведкам и технической защите информации является то, что они создаются на предприятиях выполняющих работы с использованием сведений, составляющих государственную тайну.

Режимно-секретное подразделение является основным структурным подразделением предприятия и решает задачи организации, координации и контроля деятельности других структурных подразделений (должностных лиц) по обеспечению защиты сведений, составляющих государственную тайну. На предприятиях, не выполняющих работы со сведениями, составляющими государственную тайну, для решения аналогичных задач создается и функционирует служба защиты информации (служба безопасности).

Подразделение по противодействию иностранным техническим разведкам и технической защите информации решает задачи организации и проведения комплекса технических мероприятий, направленных на исключение или существенное затруднение добывания иностранными разведками с помощью технических средств сведений, являющихся конфиденциальной информацией и подлежащих защите.

Подразделение криптографической защиты информации создается с целью закрытия каналов утечки конфиденциальной информации при ее передаче по открытым каналам (линиям) связи с использованием технических средств, а также использовании локальных вычислительных сетей, имеющих выход за пределы территории предприятия.

Подразделение охраны и пропускного режима создается с целью предотвращения несанкционированного (бесконтрольного) пребывания на территории и объектах предприятия посторонних лиц и транспорта, нанесения ущерба предприятию путем краж (хищений) с территории предприятия материальных средств и иного имущества.

Мобилизационное подразделение решает задачи всесторонней подготовки предприятия к работе в условиях военного времени, призыва и поступления мобилизационных людских и материальных ресурсов.

Кроме вышеперечисленных подразделений предприятия к работе по организации защиты информации могут привлекаться и иные структурные подразделения предприятия, основным направлением деятельности которых защита информации не является. Это - кадровые органы, органы юридической службы, органы психологической работы.

Особо необходимо отметить участие в организации защиты информации производственных, так называемых "тематических" подразделений, непосредственно создающих продукцию, товары и услуги, и, в этой связи, непосредственно взаимодействующих с другими предприятиями и органами государственной власти.

При проведении работ по организации защиты информации используются и возможности различных нештатных подразделений предприятия, в том числе коллегиальных органов (комиссий), создаваемых для решения специфических задач в этой области. Это - постоянно действующая техническая комиссия, экспертная комиссия, комиссия по рассекречиванию носителей конфиденциальной информации, комиссия по категорированию объектов автоматизации и другие.

Функции, возлагаемые на данные комиссии, будут рассмотрены в последующих главах настоящего учебного пособия, а также в ходе изучения других дисциплин.

Однако, для достижения наиболее эффективного результата при решении задач защиты конфиденциальной информации, наряду с использованием возможностей вышеупомянутых штатных и нештатных подразделений, необходимо комплексное применение имеющихся на предприятии средств защиты конфиденциальной информации.

Под средствами защиты информации понимаются технические, криптографические, программные и другие средства и системы, разработанные и предназначенные для защиты конфиденциальной информации, специальные средства, в которых они реализованы, а также

средства, устройства и системы контроля эффективности защиты информации.

Технические средства защиты информации - устройства (приборы), предназначенные для обеспечения защиты информации, исключения ее утечки, создания помех (препятствий) техническим средствам доступа к информации, подлежащей защите.

Криптографические средства защиты информации - средства (устройства), обеспечивающие защиту конфиденциальной информации путем ее криптографического преобразования (шифрования).

Программные средства защиты информации - системы защиты средств автоматизации (персональных электронно-вычислительных машин и их комплексов) от внешнего (постороннего) воздействия или вторжения.

Комплексное применение средств защиты конфиденциальной информации невозможно без четко определенной стратегии защиты информации или, методов защиты информации.

Методы защиты информации - выборочно применяемые универсальные и специфические способы (приемы, меры, мероприятия) реализации элементов системы защиты информации и входящих в них содержательных частей для формирования комплексной и индивидуальной структуры данной системы.

Общие методы защиты информации разделяются на правовые, организационно-технические и экономические. Содержание правовых методов защиты информации направлено на решение следующих задач:

- разработку, совершенствование и обеспечение функционирования механизмов отнесения сведений к информации ограниченного доступа,

засекречивания (рассекречивания) носителей информации, составляющей государственную тайну и иную охраняемую законом тайну, установления (снятия) ограничительных грифов для носителей конфиденциальной информации;

- определение перечней сведений, отнесенных к государственной (коммерческой) тайне;
- установление правового режима работы органов защиты информации;
- установление порядка доступа и допуска должностных лиц и граждан к государственной тайне и т.д.

В организационно-технических методах защиты информации рассмотрим только ее организационную составляющую, т.к. технические и экономические методы защиты информации выходят за рамки данного учебного пособия и рассматриваться не будут.

Соотношение правового обеспечения защиты информации и организационных мер ставит в зависимость деятельность по организации процесса защиты и администрированию некоторых защитных процедур от законодательства.

Законодательная система является основой разработки организационных мероприятий, и предлагает общие идеи и принципы, выраженные в нормах права, для планирования и организации деятельности, направленной на защиту конкретных сведений.

В свою очередь, организационные мероприятия являются "приемниками" правовых норм, развивают и уточняют их для конкретных условий, объектов и должностных лиц. С позиций системного подхода организация позволяет упорядочить, систематизировать любую деятельность.

Организационные методы защиты информации подразделяются по следующим классам:

- организация и соблюдение определенного порядка управленческой деятельности предприятия, направленная снижение риска утраты, утечки, модификации сведений конфиденциального характера;
- установление и соблюдение требований по организации и ведению конфиденциального делопроизводства, в том числе по размещению, оборудованию и охране;
- работа по ограничению (разграничению) круга должностных лиц предприятия по доступу к государственной тайне и конфиденциальной информации;
- осуществление принципа персональной ответственности должностных лиц за сохранность доверенной информации;
- организация подбора лиц, работающих с важной информацией их воспитание и обучение;
- систематический контроль за соблюдением режима защиты данных и оказание помощи подчиненным структурным подразделениям;
- мероприятия по сокращению оборота носителей секретной и конфиденциальной информации, систематический отбор и уничтожение ненужных носителей.

Таким образом, эффективное решение задач организации защиты информации невозможно без применения комплекса имеющихся в распоряжении руководителя предприятия методов защиты информации и соответствующих сил и средств.

8 ОТНЕСЕНИЕ СВЕДЕНИЙ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ. ЗАСЕКРЕЧИВАНИЕ И РАССЕКРЕЧИВАНИЕ СВЕДЕНИЙ.

8.1 Грифы секретности и реквизиты носителей сведений, составляющих государственную тайну.

Российской Федерации установлены три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: "особой важности", "совершенно секретно" и "секретно" Рисунок 8.1.

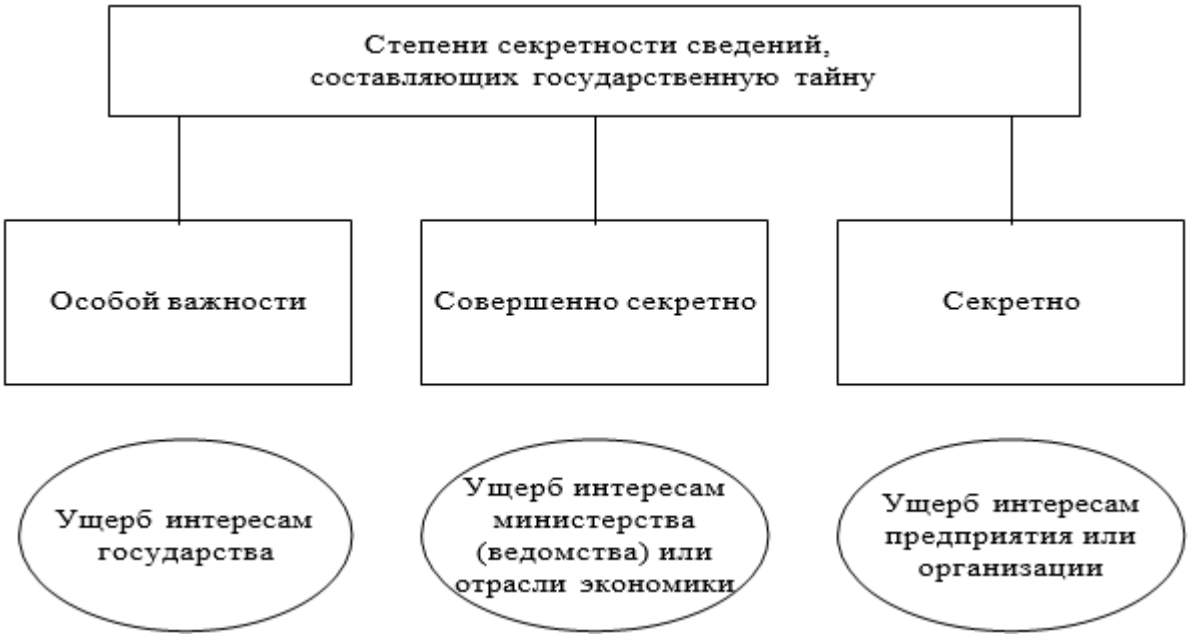

Рисунок 8.1 - Степени секретности сведений, составляющих государственную тайну.

Конкретная степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений. Она определяется руководителями органов государственной власти в развернутых перечнях сведений, подлежащих засекречиванию.

Сведения, отнесенные к государственной тайне, по степени секретности подразделяются на сведения особой важности, совершенно секретные и секретные.

К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.

К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

Носителям сведений, составляющих государственную тайну, присваивается конкретный гриф секретности.

С целью идентификации носителей сведений, составляющих государственную тайну, определения их принадлежности, обеспечения их учета и сохранности, на них наносятся реквизиты, включающие следующие данные:

- О степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в организации развернутого перечня сведений, подлежащих засекречиванию;

- Об органе государственной власти, предприятии или организации, осуществивших засекречивание носителя;
- О регистрационном номере;
- О дате или условии рассекречивания включенных в носитель сведений, составляющих государственную тайну, либо о событии, после наступления которого сведения будут рассекречены.

При невозможности нанесения таких реквизитов на носитель сведений, составляющих государственную тайну (крупногабаритное изделие, изделие, изготовленное из материала, на который нанести реквизиты невозможно), эти данные указываются в сопроводительной документации на этот носитель.

Если носитель содержит составные части с различными степенями секретности, каждой из этих составных частей присваивается соответствующий гриф секретности, а носителю в целом присваивается гриф секретности, соответствующий тому грифу секретности, который присваивается его составной части, имеющей высшую для данного носителя степень секретности сведений.

Помимо перечисленных в настоящем разделе реквизитов на носителе и (или) в сопроводительной документации к нему могут проставляться дополнительные отметки, определяющие полномочия должностных лиц по ознакомлению с содержащимися в этом носителе сведениями. Вид и порядок проставления дополнительных отметок и других реквизитов определяются нормативными документами, утверждаемыми Правительством РФ.

8.2 Отнесение сведений к государственной тайне. Засекречивание сведений и их носителей.

Под отнесением сведений к государственной тайне и их засекречиванием понимается введение, в предусмотренном Законом РФ "О государственной тайне" порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям.

Основными принципами отнесения сведений к государственной тайне и их засекречивания являются принципы законности, обоснованности и своевременности.

Законность отнесения сведений к государственной тайне и их засекречивания заключается в соответствии засекречиваемых сведений положениям статей 5 и 7 Закона РФ "О государственной тайне" и законодательству РФ о государственной тайне. Обоснованность отнесения сведений к государственной тайне и их засекречивания заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов государства, общества и граждан.

Своевременность отнесения сведений к государственной тайне и их засекречивания заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью порядком, определенным Законом РФ "О государственной тайне".

Обоснование необходимости отнесения сведений к государственной тайне в соответствии с упомянутыми принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Отнесение сведений к государственной тайне осуществляется в соответствии с "Перечнем сведений, составляющих государственную тайну", руководителями органов государственной власти, включенными в "Перечень должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне".

При этом указанные должностные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Структура "Перечня сведений, составляющих государственную тайну", представлена на Рисунке 8.2.

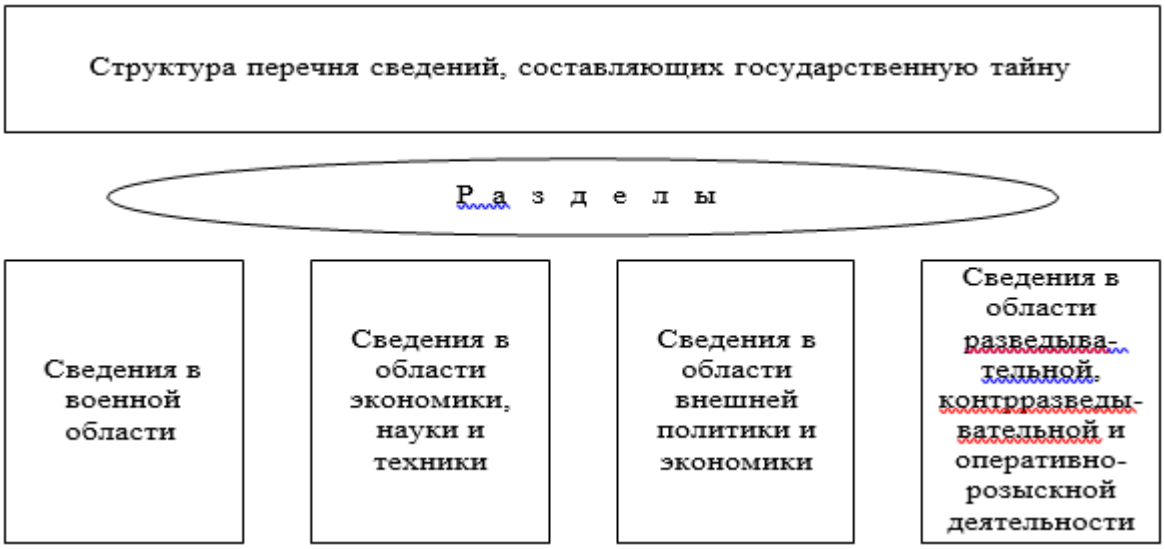

Рисунок 8.2 - Структура перечня сведений, составляющих государственную тайну.

Вместе с тем, в соответствии со статьей 7 Закона РФ "О государственной тайне", не подлежат отнесению к государственной тайне и засекречиванию сведения:

- О чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях.

- О состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности.
- О привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям.
- О фактах нарушения прав и свобод человека и гражданина;
- О размерах золотого запаса и государственных валютных резервах Российской Федерации.
- О состоянии здоровья высших должностных лиц Российской Федерации;
- О фактах нарушения законности органами государственной власти и их должностными лицами.

Руководители и должностные лица, принявшие решения о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба.

В соответствии "Перечнем сведений, составляющих государственную тайну", Межведомственная комиссия по защите государственной тайны, являющаяся органом, осуществляющим единую государственную политику в данной области, на основании предложений государственных органов формирует "Перечень сведений, отнесенных к государственной тайне". Этот перечень является открытым, в нем указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями.

Упомянутыми органами государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, в соответствии с "Перечнем сведений, отнесенных к государственной тайне", разрабатываются развернутые перечни сведений, подлежащих засекречиванию, которые действуют в данных государственных органах.

В них включаются конкретные сведения, полномочиями по распоряжению которыми наделены указанные органы, и устанавливается конкретная степень их секретности. Развернутые перечни сведений, подлежащих засекречиванию, в зависимости от их содержания могут быть открытыми или закрытыми (ограниченными для распространения).

Порядок разработки развернутых перечней и правила отнесения сведений к конкретным степеням секретности установлены "Правилами отнесения сведений, составляющих государственную тайну, к различным степеням секретности".

Основанием для засекречивания сведений и их носителей, разработанных в органе государственной власти или на предприятии (в организации), является соответствие этих сведений положениям действующего в данном органе государственной власти (на предприятии, в организации) развернутого перечня сведений, подлежащих засекречиванию. При принятии решения о засекречивании сведений их носителям присваивается соответствующий гриф секретности.

В случае невозможности идентификации данных сведений со сведениями, включенными в вышеупомянутый перечень, руководители (должностные лица) органов государственной власти (предприятий, организаций) обязаны обеспечить их предварительное засекречивание в соответствии с предполагаемой степенью секретности и присвоить их носителям гриф секретности.

Эти руководители в месячный срок после засекречивания сведений (их носителей) направляют в адрес должностного лица, утвердившего указанный развернутый перечень сведений, подлежащих засекречиванию, предложения по его дополнению (изменению).

9 ОРГАНИЗАЦИЯ АНАЛИТИЧЕСКОЙ РАБОТЫ И КОНТРОЛЯ СОСТОЯНИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ.

Анализ состояния защиты информации - это комплексное, органически взаимосвязанное изучение фактов, событий, процессов, явлений, связанных с проблемами защиты охраняемой информации; исследование данных проблем путем обработки информации о состоянии работы по выявлению возможных каналов утечки информации, о причинах и обстоятельствах, способствующих утечке и нарушениям режима секретности (конфиденциальности) в ходе повседневной деятельности предприятия.

Аналитическая работа на предприятии организуется и проводится с целью накопления, обобщения и исследования информации, материалов, фактов и событий, связанных с проблемами защиты конфиденциальной информации.

Основное предназначение аналитической работы - выработка эффективных мер, предложений и рекомендаций руководству предприятия, направленных на недопущение утечки сведений с ограниченным доступом о деятельности предприятия и проводимых работах.

Осуществляемые в ходе этой работы системное получение, анализ и накопление информации должны включать в себя элементы прогнозирования возможных действий противника по получению важной защищаемой информации.

Основными направлениями аналитической работы на предприятии являются:

- Анализ объекта защиты.
- Анализ внутренних и внешних угроз.
- Анализ возможных каналов несанкционированного доступа к информации.
- Анализ системы комплексной безопасности объектов.
- Анализ имеющих место нарушений режима конфиденциальности информации.

Функции аналитического характера на предприятии возлагаются на специально создаваемое в его структуре аналитическое подразделение, укомплектованное квалифицированными специалистами в области защиты информации. Вместе с тем, данные специалисты должны в полной мере владеть информацией по всем направлениям деятельности предприятия: знать виды, характер и последовательность выполнения производственных работ, взаимодействующие организации, специфику деятельности структурных подразделений предприятия и т.д.

Как правило, аналитическое подразделение структурно включается в состав службы безопасности предприятия.

Аналитическое подразделение должно быть единой и взаимосвязанной структурой обеспечения руководства предприятия достоверной и аналитически обработанной информацией, направленной на полноценную информационную поддержку принятия эффективных управленческих решений по всем направлениям информационной безопасности.

Основными функциями такого подразделения являются:

- Обеспечение своевременного поступления достоверной и всесторонней информации по проблемным вопросам защиты конфиденциальной информации;
- Моделирование реального сценария возможных действий предприятий-конкурентов (противника), которые могут затрагивать интересы предприятия;
- Осуществление постоянного мониторинга событий и фактов на рынке продукции, товаров и услуг, а также во внешней среде, которые могут иметь значение для деятельности предприятия;
- Обеспечение безопасности собственных информационных ресурсов;
- Обеспечение эффективности работы по анализу имеющейся информации, исключение дублирования при ее сборе, обработке и распространении;
- Подготовка выводов и предложений на основе проводимой работы в сфере информационной безопасности.

Одним из основных источников поступающей для изучения, обобщения и обработки информации являются материалы контроля состояния защиты конфиденциальной информации на предприятии.

Контроль - целенаправленная деятельность руководства и должностных лиц предприятия по проверке состояния защиты конфиденциальной информации в ходе его повседневной деятельности при выполнении предприятием всех видов работ.

Контроль состояния защиты конфиденциальной информации на предприятии организуется и проводится с целью определения истинного состояния дел по вопросам защиты информации, оценки эффективности принимаемых для исключения утечки информации мер, выявления возможных каналов утечки сведений, выработки предложений и рекомендаций руководству предприятия по совершенствованию комплексной системы защиты информации.

Указанный контроль осуществляется в порядке и в сроки, определенные нормативными правовыми актами и методическими документами, как вышестоящими органами государственной власти (министерством или ведомством), так и должностными лицами предприятия.

Организация контроля непосредственно на предприятии, в том числе входящих в его структуру подразделениях, возлагается на руководителя предприятия или его заместителя, возглавляющего работу по защите информации на предприятии.

Непосредственная организация и осуществление контроля состояния конфиденциальной информации возлагаются на службу безопасности предприятия или структурное подразделение по защите государственной тайны (режимно-секретное подразделение) предприятия.

Контроль состояния защиты конфиденциальной информации на предприятии осуществляется в форме проверок.

По характеру (способу проведения) проверки подразделяются на плановые и внезапные проверки, а по объему проведения - на комплексные и частные проверки. Плановые проверки организуются заблаговременно, включаются в соответствующие планы мероприятий предприятия на календарный год и месяц.

Внезапные проверки организуются и проводятся в необходимых случаях по указанию руководителя предприятия или его заместителя. Они могут проводиться как в масштабах предприятия, так и в его структурных подразделениях, филиалах или представительствах.

Комплексные проверки организуются и проводятся по всем направлениям защиты конфиденциальной информации. К их проведению привлекаются все структурные подразделения, отвечающие за вопросы защиты информации на предприятии. Комплексные проверки охватывают все сферы повседневной деятельности предприятия (его структурного подразделения, филиала или представительства) и имеют своей целью всестороннюю оценку состояния дел с защитой информации.

Основными задачами контроля являются:

- Проверка наличия носителей конфиденциальной информации;
- Соблюдение всеми сотрудниками предприятия норм и правил, устанавливающих порядок обращения с носителями конфиденциальной информации;
- Анализ состояния дел по вопросам защиты информации в структурных подразделениях (в том числе в филиалах и представительствах предприятия);
- Выявление угроз защите конфиденциальной информации и выработка мер по их нейтрализации;
- Оказание практической помощи должностным лицам в приведении проверяемых вопросов в соответствие требованиям нормативно-методических документов;
- Принятие мер административной и дисциплинарной ответственности к лицам, нарушающим требования по порядку обращения с носителями конфиденциальной информации;
- Проверка эффективности мер, принимаемых должностными лицами и руководителями структурных подразделений предприятия по защите конфиденциальной информации.

Особое внимание в ходе контроля уделяется вопросам хранения и обращения с носителями конфиденциальной информации на территориально обособленных объектах предприятия, находящихся на удалении.

В ходе проверки наличия носителей конфиденциальной информации проверяются: порядок учета, хранения, размножения (копирования) и уничтожения носителей конфиденциальной информации; оборудование помещений, в которых хранятся указанные носители или осуществляется работа с ними, порядок передачи носителей между исполнителями, в том числе и при убытии лиц в командировку (отпуск, на лечение), и другие вопросы.

Проверке подлежат также вопросы допуска и доступа всех категорий должностных лиц к конфиденциальной информации, в том числе и непосредственно к носителям информации, организации и осуществления пропускного и внутри-объектового режимов на предприятии, организации охраны предприятия и его объектов.

С учетом условий и специфики деятельности предприятия, осуществляемых видов деятельности, повышенное внимание уделяется вопросам защиты информации при планировании и проведении предприятием договорных работ, а также при осуществлении международного сотрудничества.

В повседневной деятельности предприятия и его структурных подразделений особое место занимают периодические проверки должностными лицами (соответствующими структурными подразделениями) наличия носителей конфиденциальной информации, проводимые порядком и в сроки, определенные нормативными правовыми актами и методическими документами, регулирующими порядок обращения с информацией различных видов конфиденциальности.

Результаты контроля доводятся до должностных лиц и сотрудников предприятия, изучаются в ходе проведения соответствующих занятий, недостатки и нарушения оперативно устраняются. Они являются основой для проведения аналитической работы и подготовки предложений руководству предприятия с целью выработки конкретных мероприятий по совершенствованию системы защиты конфиденциальной информации и повышению эффективности работы в вопросах организации и обеспечения режима секретности (конфиденциальности).

Наличие, ведение и результаты постоянной аналитической работы определяют необходимость, основы организации, структуру и содержание системы комплексной защиты информации, степень ее требуемой эффективности и направления развития и совершенствования.

От эффективности и качества ведения на предприятии аналитической работы в полной мере зависит состояние защищенности информационных ресурсов предприятия, отнесенных к категории охраняемых, а также своевременность и обоснованность принятия мер по исключению утечки конфиденциальной информации и утрат носителей конфиденциальной информации.

ЗАКЛЮЧЕНИЕ

Целью преддипломной практики является подготовка студентов к итоговой государственной аттестации (ИГА). Задачами преддипломной практики являются: сбор студентами материалов для выполнения выпускной квалификационной работы и подготовки к ИГА; закрепление и углубление в производственных условиях знаний и умений, полученных студентами при изучении общих профессиональных дисциплин и профессиональных модулей; ознакомление непосредственно на производстве с передовыми технологиями, организацией труда и экономикой производства; развитие профессионального мышления и организаторских способностей в условиях трудового коллектива. В результате пройденной преддипломной мною были приобретены профессиональные навыки и собраны материалы, которые будут применены при написании выпускной квалификационной работы.