Введение

«Кто владеет информацией - тот владеет миром» - наверно, одно из самых правдивых выражений на сегодняшний день, которое выражает всю суть самой острой проблемы в мире. За всю историю человечества можно привести тысячи примеров кражи информации, которые приводили к самым неприятным и сложным последствиям. Именно поэтому, всю информацию, представляющую хоть какую-то ценность, необходимо защищать, потому что разведывательная деятельность не спит и только совершенствуется.

Несмотря на запреты, действующие в соответствии с Российским законодательством, вероятность утечки конфиденциальной информации, реализованной с помощью современных технических средств, является вполне высокой. Техника и технологии разведки совершенствуются, и это привело к тому, что некоторые способы добычи информации уже вполне обыденные, совсем недорогие и довольно продуктивные. Следовательно, возникает необходимость комплексного пресечения всех возможных каналов утечки информации, а не только наиболее простых и доступных.

Существует несколько каналов связи, по которым передается информация, и все они должны быть защищены надлежащим образом. Что бы избежать ситуаций с утечкой информации, используются различные технические средства, которые не позволяют информации распространяться дальше заданной зоны. Если информация распространилась за пределы контролируемой зоны, то такие каналы называются каналами утечки информации. Также, существует такое понятие, как несанкционированный доступ, к нему можно отнести случаи преднамеренных искажений, кражи, удаления информации со стороны злоумышленника.

В данной работе будут рассмотрены вопросы обеспечения информационной безопасности предприятия, а также возможные угрозы безопасности помещения, предназначенного для проведения закрытых мероприятий на которых обсуждается информация, составляющая государственную тайну или конфиденциальную информацию (на примере кабинета руководителя предприятия).

Актуальностью данной работы является необходимость защиты конфиденциальных данных, информации и сведений, утеря, разглашение или искажение которых может повлечь за собой негативные последствия для организации, предприятия и государства, а также, необходимость соответствия информационной системы требованиям нормативно-правовых документов РФ.

Целью данной работы является разработка комплекса рекомендаций по обеспечению информационной безопасности на предприятии, исследование методов защиты информации от технических разведок и от ее утечки по техническим каналам, а также исследование и построение системы инженерно-технической защиты выделенного помещения, предназначенного для проведения закрытых мероприятий на которых обсуждается информация, составляющая государственную тайну или конфиденциальную информацию.

Задачи работы

Исследовать угрозы и каналы утечки информации. Рассмотреть реализацию технических мер защиты информации.

Исследовать основные мероприятия по защите информации на предприятии.
Разработать и рекомендовать политику безопасности предприятия.
Исследовать систему защиты помещения для проведения закрытых мероприятий на которых обсуждается информация, составляющая государственную тайну или конфиденциальную информацию (далее помещение). Провести анализ существующей системы инженерно-технической защиты помещения и предложить возможные варианты модернизации системы инженерно-технической защиты помещения;
Работа выполнена в интересах электронно-промышленного предприятия.
На основе общих положений работы предприятия рекомендована политика безопасности и средства ее обеспечения. В работе, на основе анализа каналов утечки информации, предложена система защиты помещения, с учетом многоканального перехвата.
Практическая значимость данной работы состоит в том, чтобы снизить риски утечки конфиденциальной информации и государственной тайны по различным каналам в рассматриваемом кабинете руководителя электронно-промышленного предприятия.

1. ОБЩИЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

информационный безопасность доступ вычислительный

1.1 Определение понятия «защита информации» и ее целей

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:
Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
Соблюдение конфиденциальности информации ограниченного доступа;
Реализацию права на доступ к информации.
На сегодняшний день можно выделить несколько видов защищаемой информации и каждый из них имеет свои особенности в области регламентации, организации и осуществления самой защиты. Стоит выделить несколько общих признаков защиты информации любого вида.
Например,
собственник информации сам организует и предпринимает меры по её защите;
защищая свою информацию, собственник ограничивает её от доступа третьих лиц, незаконного завладения или использования в ущерб своим интересам, а также сохраняет свои права на владение и распоряжение этой информацией;
для защиты информации необходимо осуществить комплекс мер по ограничению доступа к ней и создать условия, которые полностью исключат или затруднят несанкционированный доступ к засекреченной (конфиденциальной) информации и ее носителям.
Защита информации делится на решение двух основных групп задач:
а) Удовлетворение информационных потребностей, которые возникают в процессе какой-либо деятельности, то есть обеспечение специалистов организаций, фирм, предприятий секретной или конфиденциальной информацией.

Каждый специалист, в процессе работы может использовать информацию как открытого, так и закрытого типа. Информация открытого типа редко несет что-то стоящее, поэтому тут никаких ограничений нет. При снабжении специалиста засекреченной информацией действуют некоторые ограничения: наличие у этого человека соответствующего допуска (степень секретности информации, к которой он допущен) и разрешения на доступ к конкретной информации. В решении проблемы доступа специалиста к информации закрытого типа всегда существуют противоречия, с одной стороны -- необходимо максимально ограничить его доступ к засекреченной информации и тем самым снизить вероятность утечки этой информации, с другой стороны -- наиболее полно удовлетворить его потребности в информации, в том числе и засекреченной для обоснованного решения им служебных задач. В таком случае необходимо руководствоваться двумя факторами: его служебным положением и решаемой специалистом в настоящее время проблемой.

b) Ограждение засекреченной информации от несанкционированного доступа к ней в злонамеренных целях.

Эта группа, включает такие условия, как:

Создание условий эффективного использования информационных ресурсов;

Обеспечение безопасности защищаемой информации;

Сохранение секретности или конфиденциальности засекреченной информации в соответствии с установленными правилами ее защиты;

Обеспечение конституционных прав граждан на сохранение личной тайны и конфиденциальной персональной информации;

Недопущение безнаказанного растаскивания и незаконного использования интеллектуальной собственности;

Защита информационного суверенитета страны и расширение возможности государства по укреплению своего могущества за счет формирования и управления развитием своего информационного потенциала;

Виды защищаемой информации представлены на рисунке 1.

Рисунок 1. Виды защищаемой информации

1.2 Режим секретности или конфиденциальности

Понятие защита информации тесно переплетается с вопросом о режиме секретности или конфиденциальности. Режим секретности -- это осуществление системы защиты информации для определенного, конкретно заданного предприятия, фирмы, завода, лаборатории или конкретной программы, например, такой, как разработка новой продукции.

Вывод таков, что режим секретности или конфиденциальности это полный комплекс мер, выполняющий осуществление системы защиты информации, зависящий от всех факторов, которые имеют влияние на построение -- это системы защиты информации. Главная задача этого режима - обеспечение надлежащего уровня защиты информации. Всё зависит от степени её секретности, чем она выше, тем соответственно более высокий уровень защиты, и соответствующий режим секретности.

Режим секретности - реализация на конкретно заданном объекте действующих норм и правил защиты данных и сведений, включающих в себя тайну, охраняемую законом (государственную, коммерческую и т.д.), определенных и упорядоченных соответствующими законодательными нормативными актами. Группы мер, которые включает в себя режим секретности:
Разрешительную систему, а именно точное определение сотрудников, имеющих доступ к той или иной защищаемой информации и в конкретные помещения, где проводятся работы.
Осуществление пропускного режима необходимого для конкретного режима секретности, необходимой объекту.
Точно установленные правила и порядок работы с секретной документацией или иными носителям защищаемой информации.
Постоянный контроль и предупредительные работы с персоналом, имеющим доступ засекреченные информации, что помогает предотвратить её утечку.
1.3 Информационная безопасность и её цели
Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.
Другими словами, информационная безопасность - это комплекс мер, направленный на обеспечение безопасности информационных активов предприятия. Стоит подчеркнуть, что информационную безопасность можно обеспечить только в случае комплексного подхода. Рассмотрение и решение отдельных вопросов (например, технических или организационных) не решит проблему информационной безопасности предприятия целиком и полностью.
Стратегия информационной безопасности предприятия - комбинация из хорошо продуманных, запланированных действий и быстрых решений по адаптации предприятия к новым возможностям получения конкурентных преимуществ и новым угрозам ослабления её конкурентных позиций.
Главные цели информационной безопасности:
Конфиденциальность
Целостность
Пригодность
1.4 Политика информационной безопасности
Во многих российских предприятиях и компаниях дела с обеспечением информационной безопасности на низком уровне. Это подтверждают результаты статистических исследований и непосредственное общение со специалистами в данной области. Сегодня на предприятиях полноценной процедуры управления рисками информационной безопасности практически не существует. Большинство специалистов-практиков даже не берутся за эту задачу, они отдают предпочтение при решении проблем информационной безопасности руководствоваться только собственным опытом и интуицией. Убытки от нарушений информационной безопасности могут выражаться как в утечке конфиденциальной информации,

потере рабочего времени на восстановление данных, ликвидацию последствий вирусных атак, так и материальными ценностями, например, мошенничество в финансовой сфере с применением компьютерных систем.
Политика информационной безопасности - совокупность документированных управленческих решений, нацеленных на защиту информации и ассоциированных с ней ресурсов.
Политику информационной безопасности можно разделить на три уровня.
К самому высокому уровню следует отнести решения, которые касаются организации в целом и исходят от руководства организации или предприятия. Такой список может включать в себя следующие элементы:
- формирование или пересмотр программы обеспечения информационной безопасности;
- постановка целей, которые должна преследовать организация в области информационной безопасности;
- обеспечение законодательной базы;
- формулировка управленческих решений по вопросам реализации программы информационной безопасности.
Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины:
соблюдение существующих законов.
контроль действия лиц, ответственных за выработку программы безопасности.
обеспечение подчинения персонала, соответственно ввести систему поощрений и наказаний.
К среднему уровню относятся вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных систем, эксплуатируемых организацией. Например, отношение к недостаточно проверенным технологиям, использование домашних или чужих компьютеров, применение пользователями неофициального программного обеспечения и т.д.
Политика обеспечения информационной безопасности на среднем уровне должна освещать следующие темы:
Область применения;
Позиция предприятия;
Роли и обязанности;
Законопослушность;
Точки контакта;
Политика безопасности нижнего уровня можно отнести к конкретным сервисам. В нее входят цели и правила их достижения. Если сравнивать нижний уровень с двумя верхними, то он должен быть гораздо детальнее. Этот уровень очень важен для обеспечения режима информационной безопасности. Решения на этом уровне должны приниматься на управленческом, а не техническом уровне.
Политика нижнего уровня при формулировке целей может исходить из трех соображений: целостность, доступность и конфиденциальность.
Из этих целей должны быть выведены правила безопасности, которые описывают,

кто, что и при каких условиях может делать. Чем детальнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими мерами. Но и слишком жесткие правила будут мешать работе, придется тратить время на то, чтобы их пересмотреть. Руководителю в такой ситуации необходимо найти рациональное решение, компромисс, когда за приемлемую цену будет обеспечен достойный уровень безопасности, а работники не будут сильно перегружены или скованны.

2. УГРОЗЫ И КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ, МЕРЫ ЗАЩИТЫ

2.1 Классификация угроз информации

Любые данные, представляющие хоть какую-то ценность всегда находятся под угрозой несанкционированного доступа к ним, случайного или преднамеренного разрушения, или их модификации.

Существует два вида угроз данным - это естественные угрозы и искусственные угрозы.

К естественным угрозам можно отнести угрозы, вызванные воздействиями на информационную систему и ее элементы объективных физических процессов или стихийных природных явлений, которые не зависят от человеческого фактора.

К искусственным угрозам можно отнести угрозы информационной системы и ее элементам, вызванные деятельностью человека. Исходя из мотивации действий, среди искусственных угроз стоит выделить:

преднамеренные (умышленные) преследуют цель нанесения ущерба управляемой системе или пользователям. Это делается нередко злоумышленниками ради получения личной выгоды.

непреднамеренные (неумышленные, случайные). Источником таких угроз может быть выход из строя аппаратных средств, неправильные действия работников или ее пользователей, ошибки в программном обеспечении и т.д. Такие угрозы тоже следует держать во внимании, так как ущерб от них может быть значительным;

По отношению к информационной системе стоит выделить два варианта источника угроз: внешние и внутренние. Классификация угроз сохранности информации приведена на рисунке 2.Рисунок 2. Классификация угроз сохранности информации

2.2 Модель угроз безопасности информации, обрабатываемой на объекте вычислительной техники

Угроза безопасности информации - совокупность условий и факторов, создающих опасность нарушения информационной безопасности. Другими словами, это потенциальная возможность воздействия на объект защиты (преднамеренная или случайная), из-за которой может произойти потеря или утечка информации, следовательно, будет нанесен ущерб владельцу информации.

Модель угроз безопасности информации представлена на рисунке 3.

Рисунок 3. Модель угроз безопасности информации

2.3 Классификация каналов утечки информации

Каналы утечки информации -- пути и методы утечки информации из информационной системы.

а) Электромагнитный канал. Причиной его возникновения является

электромагнитное поле. Электрический ток, протекая в технических средствах обработки информации создает электромагнитное поле. Электромагнитное поле может индуцировать токи в близко расположенных проводных линиях (наводки). Электромагнитный канал в свою очередь делится на:
Радиоканал (высокочастотные излучения).
Низкочастотный канал.
Сетевой канал (наводки на провода заземления).
Канал заземления (наводки на провода заземления).
Линейный канал (наводки на линии связи между компьютерами).
b) Акустический канал. Он связан с распространением звуковых волн в воздухе или упругих колебаний в других средах, возникающих при работе устройств отображения информации.
c) Канал несанкционированного копирования.
d) Канал несанкционированного доступа.
Основные каналы утечки представлены на рисунке 4.
Рисунок 4. Основные каналы утечки информации
2.4 Каналы утечки информации на объекте вычислительной техники
2.4.1 Угроза безопасности информации через акустический канал утечки
Несанкционированный доступ к конфиденциальной информации по акустическому каналу утечки (рисунок 5) может осуществляться:
путем непосредственного прослушивания;
с помощью технических средств.
Непосредственное прослушивание переговоров (разговоров) злоумышленником может быть осуществлено:
через дверь;
через открытое окно (форточку);
через стены, перегородки;
через вентиляционные каналы.
Прослушивание переговоров через дверь возможно при условии, если вход в комнату для переговоров выполнен с нарушением требований по звукоизоляции. Не следует также вести переговоры при открытых окнах либо форточках. В этих условиях может быть непосредственный доступ к содержанию переговоров.
Стены, перегородки, потолки, да и пол комнат для ведения переговоров не являются гарантированной защитой от прослушивания, если они не проверены на звукоизоляцию и нет уверенности в том, что они отвечают требованиям по звукоизоляции.
Очень опасными с точки зрения несанкционированного доступа к содержанию переговоров являются вентиляционные каналы. Они позволяют прослушивать разговор в комнате на значительном удалении. Поэтому к оборудованию вентиляционных каналов предъявляются высокие требования.
Использование для прослушивания разговоров направленных микрофонов в настоящее время имеет широкое распространение. При этом дистанция прослушивания в зависимости от реальной помеховой обстановки может достигать

сотен метров.
В качестве направленных микрофонов злоумышленники могут использовать:
микрофоны с параболическим отражателем;
резонансные микрофоны;
щелевые микрофоны;
лазерные микрофоны.
Для прослушивания злоумышленники применяют и так называемые проводные микрофоны. Чаще всего используются микрофоны со специально проложенными проводами для передачи информации, а также микрофоны с передачей информации по линии сети 220 в.
Не исключено использование для передачи прослушиваемой информации и других видов коммуникаций (провода сигнализации, радиотрансляции, часофикации и т.д.). Поэтому при проведении всевозможных ремонтов и реконструкций на это необходимо уделять особое внимание, ибо в противном случае не исключена возможность внедрения таких подслушивающих устройств. Широкое применение у злоумышленников для прослушивания переговоров (разговоров) находят радиомикрофоны. В настоящее-время их насчитывается более 200 различных типов. Обобщенные характеристики радиомикрофонов следующие:
- диапазон частот: 27 - 1500 мГц;
- вес: единицы грамм - сотни грамм;
- дальность действия: 10 - 1600м;
- время непрерывной работы: от нескольких часов-до нескольких лет (в зависимости от способа питания).
Данные устройства представляют собой большую угрозу безопасности ведения переговоров (разговоров). Поэтому необходимо делать все возможное для исключения их наличия в комнатах для переговоров.
В последнее десятилетие злоумышленники стали применять устройства, позволяющие прослушивать разговоры в помещениях на значительном удалении от них (из других районов, городов и т.д.), используя телефонные линии.Рисунок 5. Модель угроз информации через акустический канал утечки
2.4.2 Угроза безопасности информации за счет высокочастотного Навязывания
Сущность прослушивания переговоров с помощью высокочастотного навязывания состоит в подключении к телефонной линии генератора частоты и последующего приема «отраженного» от телефонного аппарата промодулированного ведущимся в комнате разговором сигнала.
Таким образом, анализ угроз конфиденциальной информации, которые содержатся при ведении переговоров (разговоров) показывает, что если не принять мер защиты, то возможен доступ злоумышленников к ее содержанию.Рисунок 6. Модель угроз информации за счет высокочастотного навязывания
2.4.3 Угроза безопасности информации по оптическому каналу утечки
Если переговоры ведутся в комнате, где окна не оборудованы шторами, жалюзями, то в этом случае у злоумышленника появляется возможность с помощью оптических приборов с большим усилением (бинокли, подзорные трубы) просматривать

помещение. Видеть, кто в нем находится и что делает.
стекло
Лазерный
луч
Рисунок 7. Модель угроз информации по оптическому каналу
2.4.4 Угроза безопасности информации через виброакустический канал утечки
Несанкционированный доступ к содержанию переговоров (разговоров) злоумышленниками может быть также осуществлен (рисунок 8) с помощью стетоскопов и гидроакустических датчиков.Рисунок 8. Модель угроз информации через виброакустический канал утечки
С помощью стетоскопов возможно прослушивание переговоров (разговоров) через стены толщиной до 1 м 20 см (в зависимости от материала).
В зависимости от вида канала передачи информации от самого вибродатчика стетоскопы подразделяются на:
- проводные (проводной канал передачи);
- радио (канал передачи по радио);
- инфракрасные (инфракрасный канал передачи).
Не исключена возможность использования злоумышленниками и гидроакустических датчиков, позволяющих прослушивать разговоры в помещениях, используя трубы водообеспечения и отопления.
2.4.5 Угрозы безопасности информации, вызванные умышленными факторами
Угрозы, вызванные умышленными факторами, могут исходить как со стороны недобросовестных сотрудников организации (лиц, имеющих доступ на объект вычислительной техники (ВТ), пользователей), так и со стороны посторонних лиц (злоумышленников). Некоторые виды умышленных угроз могут быть отнесены к обоим признакам, однако, рассматривать их целесообразно отдельно.
Угрозы, исходящие со стороны пользователей.
К этому виду угроз относятся:
использование штатного способа доступа к системе с целью навязывания запрещенных действий (нештатное изменение атрибутов доступа);
маскировка под истинного пользователя путем навязывания характеристик его авторизации (использование подобранных или подсмотренных паролей, ключей шифрования, похищенных идентификационных карточек, пропусков и т. п.);
маскировка под истинного пользователя после получения им доступа;
использование служебного положения для получения привилегированного доступа к информации (на объект ВТ) или отмены ограничений, обусловленных требованиями по защите информации;
физическое разрушение системы или вывод из строя ее компонентов;
отключение или вывод из строя подсистем обеспечения безопасности информации;
хищение носителей информации и несанкционированное их копирование;
чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств (просмотр «мусора»);
внедрение аппаратных и программных “закладок”, “вирусов” и “троянских”

программ, позволяющих скрытно и незаконно получать информацию с объекта ВТ или получать доступ к модификации (уничтожению) информации обрабатываемой на объекте ВТ.
Угрозы, исходящие со стороны посторонних лиц (злоумышленников).
В эту категорию угроз входят:
маскировка под истинного пользователя путем навязывания характеристик его авторизации (использование подобранных или подсмотренных паролей, ключей шифрования, похищенных идентификационных карточек, пропусков и т. п.);
маскировка под истинного пользователя после получения им доступа;
подкуп или шантаж персонала, имеющего определенные полномочия;
хищение носителей информации;
внедрение аппаратных и программных “закладок”, “вирусов” и “троянских” программ, позволяющих скрытно и незаконно получать информацию с объекта ВТ или получать доступ к модификации (уничтожению) информации обрабатываемой на объекте ВТ;
незаконное подключение к линиям связи;
перехват данных, передаваемых по каналам связи;
перехват информации за счет закладных устройств;
анализ паразитных излучений аппаратуры.
2.5 Реализация технических мер защиты информации на объекте ВТ
Для реализации первичных технических мер защиты требуется обеспечить:
* блокирование каналов утечки информации и несанкционированного доступа к ее носителям;
* проверку исправности и работоспособность технических средств объекта ВТ;
* установить средства выявления и индикации угроз, проверить их работоспособность;
* установить защищенные средства обработки информации, средства защиты информации и проверить их работоспособность;
* применить программные средства защиты в средствах вычислительной техники, автоматизированных системах, осуществить их функциональное тестирование и тестирование на соответствие требованиям защищенности;
* использовать специальные инженерно-технические сооружения и средства (системы).
Выбор средств обеспечения защиты информации обусловлен фрагментарным или комплексным способом защиты информации.
Фрагментарная защита обеспечивает противодействие определенной угрозе.
Комплексная защита обеспечивает одновременное противодействие множеству угроз.
Блокирование каналов утечки информации может осуществляться:
* демонтажем технических средств, линий связи, сигнализации и управления, энергетических сетей, использование которых не связано с жизнеобеспечением предприятия и обработкой информации;
* удалением отдельных элементов технических средств, представляющих собой

среду распространения полей и сигналов, из помещений, где циркулирует информация;
* временным отключением технических средств, не участвующих в обработке информации, от линий связи, сигнализации, управления и энергетических сетей;
* применением способов и схемных решений по защите информации, не нарушающих основные технические характеристики средств обеспечения информационных данных.
Блокирование несанкционированного доступа к информации или ее носителям может осуществляться:
* созданием условий работы в пределах установленного регламента;
* исключением возможности использования не прошедших проверку (испытания) программных, программно-аппаратных средств.
Средства выявления и индикации угроз применяются для сигнализации и оповещения владельца (пользователя, распорядителя) информации об утечке информации или нарушении ее целостности. Средства защиты информации применяются для пассивного или активного скрытия информации.
Для пассивного скрытия применяются фильтры-ограничители, линейные фильтры, специальные абонентские устройства защиты и электромагнитные экраны.
Для активного скрытия применяются узкополосные и широкополосные генераторы линейного и пространственного зашумления.
Программные средства применяются для обеспечения:
* идентификации и аутентификации пользователей, персонала и ресурсов системы обработки информации;
* разграничения доступа пользователей к информации, средствам вычислительной техники и техническим средствам автоматизированных систем;
* целостности информации и конфигурации автоматизированных систем;
* регистрации и учета действий пользователей;
* маскирования обрабатываемой информации;
* реагирования (сигнализации, отключения, приостановки работ, отказа в запросе) на попытки несанкционированных действий.
По результатам выполнения рекомендаций акта обследования и реализации мер защиты информации следует составить в произвольной форме акт приемки работ по защите информации, который должен быть подписан исполнителем работ, лицом, ответственным за защиту информации, и утвержден руководителем предприятия.
Для определения полноты и качества работ по защите информации следует провести аттестацию. Аттестация выполняется организациями, имеющими лицензии на право деятельности в области защиты информации. Объектами аттестации являются компоненты информационной системы и их отдельные элементы, в которых циркулирует информация, подлежащая технической защите. В ходе аттестации требуется:
- установить соответствие аттестуемого объекта требованиям защиты информации;
- оценить качество и надежность мер защиты информации;
- оценить полноту и достаточность технической документации для объекта

аттестации;
- определить необходимость внесения изменений и дополнений в организационно-распорядительные документы.
Технические меры по защите информации на объекте ВТ должны предусматривать:
Ограничение доступа внутрь корпуса компьютера путем установления механических запорных устройств.
Уничтожение всей информации на винчестере компьютера при ее отправке в ремонт с использованием средств низкоуровневого форматирования.
Организацию питания компьютера от отдельного источника питания или от общей (городской) электросети через стабилизатор напряжения (сетевой фильтр) или мотор-генератор.
Использование для отображения информации жидкокристаллических или плазменных дисплеев, а для печати - струйных или лазерных принтеров.
Размещение дисплея, системного блока, клавиатуры и принтера на расстоянии не менее 2,5-3,0 метров от устройств освещения, кондиционирования воздуха, связи (телефона), металлических труб, телевизионной и радиоаппаратуры, а также других компьютеров, не использующихся для обработки конфиденциальной информации.
Отключение компьютера от локальной сети или сети удаленного доступа при обработке на ней конфиденциальной информации, кроме случая передачи этой информации по сети.
Установка принтера и клавиатуры на мягкие прокладки с целью снижения утечки информации по акустическому каналу.
Во время обработки ценной информации на компьютере рекомендуется включать устройства, создающие дополнительный шумовой фон (кондиционеры, вентиляторы), а также обрабатывать другую информацию на рядом стоящих компьютерах. Эти устройства должны быть расположены на расстоянии не менее 2,5-3,0 метров.
Уничтожение информации непосредственно после ее использования.

3. ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

3.1 Задачи и принципы организации службы информационной безопасности

На многих предприятиях организуют отделы службы безопасности. В обязанности такой службы входит организация защиты сведений, непосредственно связанных с государственной и коммерческой тайной, обучение сотрудников хранить секреты своей фирмы, разъяснение правил соблюдения защиты информации и политики конфиденциальности фирмы, создание методических документов. Служба безопасности собирает всё необходимое о наличии секретной информации, сроках её хранения, коммерческой тайне данного предприятия, определяет круг лиц, имеющих к ней доступ и контролирует его, чтобы доступ был обеспечен только тем сотрудникам, которым она нужна непосредственно по службе. Так же на службу безопасности обычно возложены такие обязанности, как отслеживание информации о состоянии рынка, конкурентах, анализировать и контролировать попытки конкурирующих фирм получить доступ к защищаемой информации, а также уметь четко и быстро устранять недостатки в области защиты коммерческой тайны.

Организуется специальная система доступа к конфиденциальной информации - целый комплекс административно-правовых норм, организующий доступ информации исполнителями или руководителем секретных работ. Целью этой системы является обезопасить работу от несанкционированного получения секретной информации. Подразделяется эта система на:
разрешительную систему доступа к секретной документации;
систему шифров и пропусков для доступа в помещения, где ведутся секретные работы.
Обеспечивает физическую сохранность носителей секретной информации и предотвращение доступа посторонних на территорию секретных работ система охраны. Система охраны - комплекс мероприятий, средств, сил и мероприятий, преграждающих доступ посторонних к защищаемой информации.
Комплекс мер, направленных на защиту конфиденциальной информации, осуществляемый руководством, администрацией и системой безопасности, это:
ежедневный контроль над соблюдением сотрудниками правил защиты информации;
соблюдение всеми сотрудниками правил внутреннего распорядка, пожарной безопасности, инструкций по защите сведений и т.д.;
контроль над прохождением на территорию посторонних лиц и отслеживание их передвижений;
выявления каналов утечки информации и меры по их перекрытию;
предотвращение разглашения защищаемой информации в открытых публикациях;
работа с клиентами, ведение переговоров с партнерами и т.д., важно заключение взаимовыгодных соглашений, а не получение информации о защищаемой информации.
Правовая защита информации.
Правовые меры, регулирующие вопросы защиты секретной и конфиденциальной информации, делят на две группы:
нормативные акты, регламентирующие правила и процедуры защиты информации;
нормативные акты, устанавливающие ответственность за покушение на сведения.
Уголовно-правовые нормы по своему содержанию являются, с одной стороны, запрещающими, то есть они под страхом применения мер уголовного наказания запрещают гражданам нарушать свои обязанности и совершать преступления, а с другой стороны, они обязывают соответствующие органы государства (ФСБ, МВД, прокуратуру) привлечь лиц, виновных в совершении преступления, к уголовной ответственности.Кроме того, нарушения режима секретности, правил сохранения государственной и коммерческой тайны, не являющиеся преступлением, могут повлечь материальное, дисциплинарное или административное взыскание в соответствии с действующими нормативными актами: отстранение от работы, связанной с секретами или перевод на другую работу, менее оплачиваемую и тоже не связанную с засекреченной информацией.
Организационная защита информации.
Эта группа мер преследует цель организации работы по выполнению правил, процедур и требований защиты государственной и коммерческой тайны на основе

правил, установленных законами и подзаконными правовыми актами (инструкциями, положениями и т.п.).
Организационные меры по защите информации подразумевают, прежде всего, работу с кадрами, которые будут осуществлять мероприятия по защите информации, обучение сотрудников правилам защиты засекреченной информации. Нормативно-правовые организационные режимные меры-это основа для решения вопрос защиты информации о соблюдение принципа максимального ограничения числа лиц, которые имеют к секретным работам и документам. Организационные меры защиты информации требуют детального соблюдения правил секретного делопроизводства, чтобы исключить или свести к минимуму утрату секретных документов. Основное назначение организационных мер защиты информации -- предупредить несанкционированный доступ к государственным или коммерческим секретам и утечку защищаемой информации.
Инженерно-техническая защита информации.
Это отдельное направление защиты информации. Развитие технических средств разведки (ТСР) потребовало от государства создания целой системы мер противодействия сбору разведывательной информации с помощью ТСР. Инженерно-технические меры защиты информации -- это комплекс организационных и инженерно-технических мероприятий, направленных на исключение или существенное затруднение добыванию с помощью ТСР защищаемой информации. Главное здесь, что каждое действие требует противодействие. Противостоять ТСР с помощью только организационных режимных мер явно недостаточно, так как ТСР не знают границ и на их деятельность не влияют погодные условия.
Инженерно-технические меры защиты информации делятся на три группы:
Обще предупредительные меры, включающие правовое регулирование использования технических средств в процессе осуществления международных связей; установление и поддержание режимов, направленных на предотвращение утечки защищаемой информации по каналам, доступным ТСР и др.;
организационные меры включают в себя такие мероприятия, как анализ и обобщение информации о ТСР и выработка путей защиты этих параметров;
технические меры включают комплекс инженерно-технических средств и мероприятий, используемых для скрытия от ТСР защищаемых сведений об объектах защиты и технической дезинформации соперника.
3.2 Охраняемые сведения и объекты защиты информации предприятия
Целью мероприятий по защите информации, проводимых на объектах предприятия, является снижение риска получения ущерба в условиях действия преднамеренных и непреднамеренных угроз информационной безопасности. Достижение требуемого уровня информационной безопасности должно быть обеспечено системным применением организационных, организационно-технических, технических и программно-технических мер на всех этапах эксплуатации объектов предприятия. Указанная цель достигается путем рационального и взаимосвязанного решения на объектах предприятия следующих задач, увязанных единым замыслом:

a. определения сведений, информационных ресурсов и процессов, которые необходимо защитить;
b. анализа демаскирующих признаков, раскрывающих охраняемые сведения об объектах защиты, каналов утечки, хищения, несанкционированного доступа и воздействия на защищаемую информацию;
c. оценки возможностей технических разведок и криминальных структур по получению защищаемой информации, несанкционированному доступу и воздействию на информационные ресурсы и процессы, оценки реальной опасности утечки информации, искажения, модификации, уничтожения или блокирования информационных ресурсов и процессов;
d. разработки и внедрения технически и экономически обоснованных мероприятий по защите информации с учетом выявленных возможных каналов ее утечки, воздействий и доступа;
e. организации и проведения контроля эффективности защиты информации на объектах информатизации предприятия.
К охраняемым сведениям, защищаемым информационным ресурсам и процессам на всех этапах жизненного цикла объектов предприятия относятся:
a) Речевая информация, содержащая сведения, отнесенные к государственной тайне.
b) Информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, представленные в виде носителей на магнитной и оптической основе, информативных электрических сигналов, электромагнитных полей, информационных массивов и баз данных.
При анализе безопасности охраняемых сведений и информационных ресурсов, должны рассматриваться все возможные виды угроз.
Подлежащие защите объекты информатизации предприятия по требованиям обеспечения информационной безопасности относятся к одной из трех групп:
a. Первая группа - основные технические средства и системы, а также их комплектующие с помещениями, в которых они размещены.
b. Вторая группа - выделенные помещения, специально предназначенные для проведения закрытых мероприятий на которых обсуждается информация, составляющая государственную тайну, а также оборудованные средствами правительственной связи и иных видов специальной связи
c. Третья группа - вспомогательные технические средства и системы, установленные в выделенных помещениях.
К основным техническим средствам относятся:
a) Отдельные автоматизированные рабочие места структурных подразделений предприятия, предназначенные для обработки информации, содержащей сведения, составляющие государственную тайну.
b) Средства обработки речевой, графической, видео информации, используемой для обработки секретной информации.
c) Средства для изготовления и размножения секретных документов.
d) Средства и системы связи, в которых циркулирует секретная информация.
К выделенным помещениям III категории относятся служебные кабинеты и рабочие

комнаты подразделений предприятия, в которых проводятся обсуждения и переговоры по вопросам со степенью секретности не выше «секретно», а также актовые залы, предназначенные для закрытых мероприятий.
К выделенным помещениям II категории относятся помещения, специально выделенные для проведения совещаний по совершенно секретным вопросам, а также служебные кабинеты руководящего состава предприятия и основных его подразделений в которых могут вестись обсуждения и переговоры по совершенно секретным вопросам.
К вспомогательным относятся технические средства и системы, не предназначенные для обработки, передачи и хранения секретной информации, размещенные в выделенных помещениях, а также совместно с основными техническими средствами и системами.
3.3 Организационные и технические мероприятия по защите информации
Защита информации на объектах предприятия должна осуществляться посредством выполнения комплекса мероприятий, направленных на: скрытие или существенное затруднение добывания с помощью технических средств разведки охраняемых сведений об объектах защиты; предотвращение утечки информации или воздействия на информационные ресурсы и процессы по техническим каналам и за счет несанкционированного доступа к ним; предупреждение преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации (информационных технологий) в процессе ее обработки, передачи и хранения или нарушения работоспособности технических средств.
Исходя из перечня основных угроз информационной безопасности, в комплексе мероприятий по защите информации на объектах предприятия можно выделить несколько направлений:
Защита от утечки по техническим каналам секретной речевой (акустической) информации, обсуждаемой в помещениях объектов предприятия.
Защита основных технических средств и систем от утечки информации, составляющей государственную тайну, по каналам побочных электромагнитных излучений и наводок
Защита информации от несанкционированного доступа, в том числе от компьютерных вирусов и других программно-технических воздействий, от хищения технических средств с находящейся в них информацией или отдельных носителей информации.
Защита информации от воздействия источников дестабилизирующих (разрушающих) электромагнитных излучений, а также от уничтожения и искажения информации через специально внедренные электронные и программные средства (закладки).
Организация защиты от утечки по техническим каналам секретной речевой (акустической) информации предполагает проведение комплекса организационно-технических мероприятий, направленных на устранение акустического и виброакустического каналов утечки информации, а также технических каналов,

возникающих при эксплуатации вспомогательных технических средств и за счет внедрения электронных устройств перехвата информации.
К таким мероприятиям относятся:
Категорирование помещений предприятия, используемых для обсуждения информации, составляющей государственную тайну.
Проведение специальной проверки выделенных помещений, а также размещенных в них технических средств иностранного производства с целью выявления возможно внедренных в них электронных устройств перехвата информации (закладок).
Выполнение организационно-режимных мероприятий по допуску и охране выделенных помещений.
Установка в выделенных помещениях технических средств (оконечных устройств телефонной связи, радиотрансляции, сигнализации, электрочасофикации и т.д.), сертифицированных по требованиям безопасности информации либо защищенных по результатам специальных исследований сертифицированными средствами защиты.
Исключение использования в выделенных помещениях радиотелефонов, оконечных устройств сотовой связи.
Выполнение требований по звукоизоляции и виброакустической защите ограждающих конструкций выделенных помещений, их систем вентиляции и кондиционирования. Повышение звукоизоляции ограждающих конструкций помещений или установка активных средств защиты проводятся по результатам проведенных измерений отношения информативный сигнал/шум в местах возможного перехвата информации.
Оформление технических паспортов по вопросам защиты информации на выделенные помещения осуществляет главный специалист по информационной безопасности предприятия с привлечением подразделений, эксплуатирующих здания, системы электроснабжения, коммуникации и технические средства, а также подразделений, располагающихся в выделенных помещениях.
Организация и проведение аттестации выделенных помещений по требованиям безопасности информации с оформлением "Аттестата соответствия". Аттестация проводится организацией, имеющей соответствующую лицензию ФСТЭК России.
В целях защиты информации, обрабатываемой всеми видами основных технических средств и систем, организуется и проводится комплекс организационно-технических мероприятий, направленный на исключение или существенное снижения уровня побочных электромагнитных излучений и наводок в линиях связи и коммуникациях, имеющих выход за пределы контролируемой зоны объектов предприятия.
К таким мероприятиям относятся:
Категорирование основных технических средств и систем.
Проведение специальной проверки основных технических средств иностранного производства с целью выявления возможно внедренных в них электронных устройств перехвата информации (закладок).
Проведение специальных исследований основных технических средств и систем и выдача предписания на эксплуатацию.

Выполнение требований предписаний на эксплуатацию по размещению основных технических средств и систем относительно границ контролируемой зоны.
Выполнение требований предписаний на эксплуатацию по размещению основных технических средств и систем относительно вспомогательных технических средств и систем, имеющих выход за пределы контролируемой зоны.
Выполнение требований предписаний на эксплуатацию по защите системы электропитания основных технических средств и систем.
Выполнение требований предписаний на эксплуатацию по защите системы заземления основных технических средств и систем.
Оформление технических паспортов по вопросам защиты информации на основные технические средства и системы осуществляет главный специалист по информационной безопасности предприятия совместно с подразделением, эксплуатирующим данные средства.
В целях защиты информации и информационных процессов (технологий) в системах информатизации (автоматизированных системах) проводятся мероприятия по их защите от несанкционированного доступа и программно-технических воздействий, в том числе от компьютерных вирусов. Защите подлежат автоматизированные системы, предназначенные для обработки информации, составляющей государственную тайну.
Мероприятия по защите автоматизированных систем, предназначенных для обработки информации, составляющей государственную тайну, от несанкционированного доступа к информации направлены на достижение трех основных свойств защищаемой информации: конфиденциальность, целостность, доступность.
Мероприятия по защите информации при нахождении на объектах предприятия иностранных представителей, порядок их реализации и ответственность должностных лиц за их выполнение определяются отдельной инструкцией о приеме иностранных граждан.
Мероприятия по обеспечению информационной безопасности выполняются на всех этапах жизненного цикла объектов предприятия и являются неотъемлемой частью работ по их созданию и эксплуатации.
На стадии эксплуатации объекта предприятия, системы информатизации и средств защиты информации в ее составе осуществляются:
Администрирование систем информатизации и связи с целью обеспечения информационной безопасности при их эксплуатации, в том числе:
управление доступом в систему и к ее элементам;
формирование и распределение реквизитов полномочий пользователей в соответствии с установленными правилами разграничения доступа;
формирование и распределение ключевой и парольной информации;
регистрация и учет действий в системе;
учет носителей информации;
обеспечение сигнализации о попытках нарушения защиты;
поддержание функционирования криптографической подсистемы защиты

информации;
поддержание функционирования технических и программных средств и систем защиты информации в установленных эксплуатационной документацией режимах;
контроль целостности эксплуатируемого на средствах вычислительной техники программного обеспечения с целью выявления несанкционированных изменений в нем, а также выполнения мероприятий по антивирусной защите носителей информации и сообщений, получаемых по каналам связи;
инструктаж персонала и пользователей технических средств передачи, обработки и хранения информации по правилам работы со средствами защиты информации;
участие в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации.
Организация и контроль эксплуатации средств физической защиты, исключающих несанкционированный доступ к объектам защиты и техническим средствам, их хищение и нарушение работоспособности.
Периодическая проверка помещений на отсутствие возможно внедренных радиоэлектронных средств перехвата информации.
Периодическое обследование выделенных помещений, средств и систем информатизации.
Периодическая проверка автоматизированных рабочих мест на выполнение требований по антивирусной защите.
Периодическая аттестация объектов защиты.
Контроль проведения ремонтных и сервисных работ в выделенных помещениях, а также на технических средствах и их коммуникациях
3.4 Программно-технические методы и средства защиты информации от несанкционированного доступа на объекте ВТ
Технической основой системы защиты информации от несанкционированного доступа являются программно-технические методы и средства.
Для того чтобы сформировать оптимальный комплекс программно-технических методов и средств защиты информации, необходимо пройти следующие этапы:
Определение информационных и технических ресурсов, подлежащих защите;
Выявление полного множества потенциально возможных угроз и каналов утечки;
Проведение оценки уязвимости информации для выявленных угроз и каналов утечки;
Определение требований к системе защиты информации;
Осуществление выбора средств защиты информации и их характеристик;
Внедрение и организация использования выбранных мер, способов и средств защиты;
Осуществление контроля целостности и управление системой защиты.
Совокупность защитных методов и средств включает в себя:
Программные средства и методы;
Аппаратные средства;
Защитные (криптографические) преобразования;
Организационные мероприятия.

Программные методы защиты - это совокупность алгоритмов и программ, обеспечивающих разграничение доступа и исключение несанкционированного использования информации.
Сущность аппаратной или схемной защиты состоит в том, что в устройствах и технических средствах обработки информации предусматривается наличие специальных технических решений, обеспечивающих защиту и контроль информации, например, экранирующие устройства, локализующие электромагнитные излучения или схемы проверки информации на четность, осуществляющей контроль правильности передачи информации между различными устройствами информационной системы.