Министерство цифрового развития, связи и   
массовых коммуникаций Российской Федерации

Сибирский государственный университет телекоммуникаций и информатики

# Контрольная работа

# по дисциплине: Основы информационной безопасности

**Анализ физических/технических средств обеспечения информационной безопасности**

Выполнила: Штрезер Д.А.

Группа: МБ-12

Тема: 27

Проверил: Киселев А.А.

Новосибирск, 2025 год

СОДЕРЖАНИЕ

[Введение 2](#_Toc95651803)

[1.Физическая защита информации 3](#_Toc95651804)

[2. Характеристика физических средств защиты 8](#_Toc95651805)

[3.Анализ технических средств обеспечения информационной безопасности 16](#_Toc95651809)

[Заключение 21](#_Toc95651810)

[Список литературы 24](#_Toc95651811)

**Введение**

Информационная безопасность (ИБ) – это состояние информационной системы, при котором она наименее восприимчива к вмешательству и нанесению ущерба со стороны третьих лиц. Безопасность данных также подразумевает управление рисками, которые связаны с разглашением информации или влиянием на аппаратные и программные модули защиты.

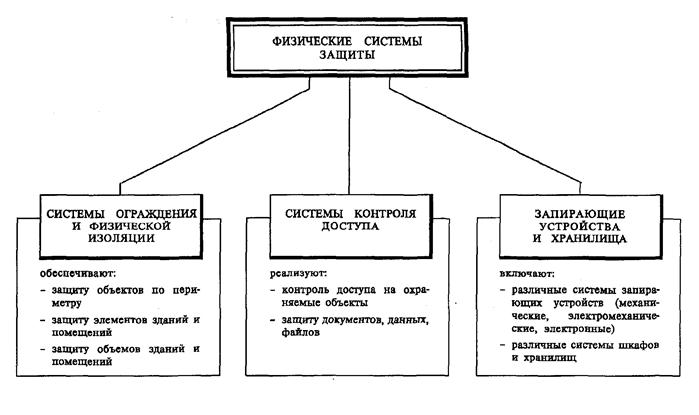
Физические средства защиты – это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.

Вопросы технического обеспечения информационной безопасности предприятия решают не только ИТ-подразделения. В безопасном использовании информационных ресурсов заинтересовано руководство и другие службы компании.

Работа состоит из введения, основной части, заключения, списка литературы.

**1.Физическая защита информации**

**Физические средства защиты –**это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.



К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий (рисунок).

Эти средства применяются для охраны:

1) территории предприятия и наблюдение за ней;

2) зданий, внутренних помещений и контроль за ними;

3) оборудования, продукции, финансов и информации;

4) осуществление контролируемого доступа в здания и помещения.

Все физические средства защиты объектов можно разделить на **три категории**:

* средства предупреждения,
* средства обнаружения и
* системы ликвидации угроз.

Охранная сигнализация и охранное телевидение, например, относятся к средствам обнаружения угроз; заборы вокруг объектов – это средства предупреждения несанкционированного проникновения на территорию, а усиленные двери, стены, потолки, решетки на окнах и другие меры служат защитой и от проникновения, и от других преступных действий (подслушивание, обстрел, бросание гранат и взрывпакетов). Средства пожаротушения относятся к системам ликвидации угроз.

**По физической природе и функциональному назначению** средства защиты объектов можно разделить на следующие группы:

– охранные и охранно-пожарные системы;

– охранное телевидение;

– охранное освещение;

– средства физической защиты.

**Охранные системы** предназначены для

* обнаружения попыток проникновения на объект защиты;
* оповещения сотрудников охраны о появлении угроз.

К элементам охранных систем относятся датчики, принципы работы которых определяют возможности охранных систем. Уже разработано и широко используется значительное количество самых разнообразных датчиков, как по принципам обнаружения различных физических полей, так и по тактическому использованию. Датчики посредством тех или иных каналов связи соединены с контрольно-приемным устройством пункта (или поста) охраны и средствами тревожного оповещения.

**Охранное телевидение** позволяет контролировать обстановку как на объекте, так и вокруг него в динамике ее развития, определять опасность действий, вести скрытое наблюдение и производить видеозапись для последующего анализа правонарушения как с целью анализа, так и для привлечения к ответственности нарушителя.

Источниками изображения (датчиками) в системах охранного телевидения являются видеокамеры. Через объектив изображение злоумышленника попадает на светочувствительный элемент камеры, в котором оно преобразуется в электрический сигнал, поступающий затем по специальному коаксиальному кабелю на монитор и при необходимости – на видеомагнитофон.

Обязательной составной частью системы защиты любого объекта является **охранное освещение**. Различают дежурное и тревожное охранное освещение.

К средствам **физической защиты** относятся:

– естественные и искусственные барьеры;

– особые конструкции периметров, оконных и дверных переплетов,;

– зоны безопасности.

Важным средством физической защиты является планировка объекта, его зданий и помещений по **зонам безопасности**, которые учитывают степень важности различных частей объекта, с точки зрения нанесения ущерба от различного вида угроз.

Среди средств **физической защиты** особо следует отметить **средства защиты ПЭВМ** от хищения и проникновения к их внутренним компонентам. Для этого используют металлические конструкции с клейкой подставкой, которая обеспечивает сцепление с поверхностью стола с силой в 2500-2700 кг/см. Это исключает изъятие или перемещение ПЭВМ без нарушения целостности поверхности стола. Перемещение ПЭВМ возможно только с использованием специальных ключей и инструментов.

*2. Физическая защита данных*

Физическая защита данных включает в себя защиту

1. Кабельной системы

2. Системы электроснабжения

3.Системы архивирования и дублирования информации

4.Защиту от стихийных бедствий

**1. Кабельная система** остается главной "ахиллесовой пятой" большинства локальных вычислительных сетей: по данным различных исследований, именно кабельная система является причиной более чем половины всех отказов сети. В связи с этим кабельной системе должно уделяться особое внимание с самого момента проектирования сети.

Наибольшее распространение в настоящее время получили следующие стандарты кабельных систем:

Спецификации корпорации IBM, которые предусматривают девять различных типов кабелей. Наиболее распространенным среди них является кабель IBM type 1 - экранированная витая пара (STP) для сетей Token Ring.

Система категорий Underwriters Labs (UL) представлена этой лабораторией совместно с корпорацией Anixter. Система включает пять уровней кабелей. В настоящее время система UL приведена в соответствие с системой категорий EIA/TIA.

Стандарт EIA/TIA 568 был разработан совместными усилиями UL, American National Standards Institute (ANSI) и Electronic Industry Association/Telecommunications Industry Association, подгруппой TR41.8. 1 для кабельных систем на витой паре (UTP).

В дополнение к стандарту EIA/TIA 568 существует документ DIS 1 180i, разработанный International Standard Organisation (ISO) и International Electrotechnical Commission (IEC). Данный стандарт использует термин "категория" для отдельных кабелей и термин "класс" для кабельных систем.

**2.** **Системы электроснабжения.**Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии в настоящее время является установка **источников бесперебойного питания**. Большинство источников бесперебойного питания одновременно выполняет функции и стабилизатора напряжения, что является дополнительной защитой от скачков напряжения в сети. Многие современные сетевые устройства - серверы, концентраторы, мосты и т. д. - оснащены собственными дублированными системами электропитания.

**3.** **Системы архивирования и дублирования информации.**Организация надежной и эффективной системы архивации данных является одной из важнейших задач по обеспечению сохранности информации в сети. В небольших сетях, где установлены один-два сервера, чаще всего применяется установка системы архивации непосредственно в свободные слоты серверов. В крупных корпоративных сетях наиболее предпочтительно организовать выделенный специализированный архивационный сервер. Среди наиболее распространенных моделей архивационных серверов можно выделить Storage Express System корпорации Intel, ARCserve for Windows, производства фирмы Cheyenne и ряд других.

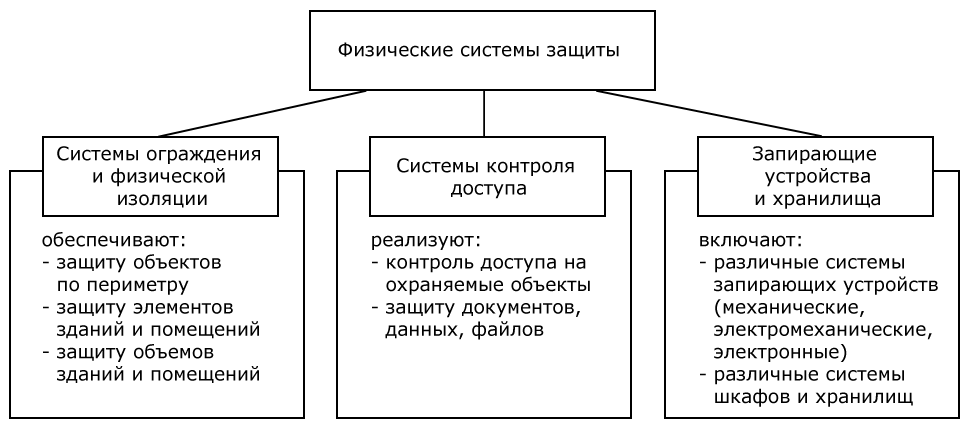
Организация дисковых массивов предусматривает различные технические решения, реализованные на нескольких уровнях.

Уровень 0 предусматривает простое разделение потока данных между двумя или несколькими дисками. Преимущество подобного решения заключается в увеличении скорости ввода/вывода пропорционально количеству задействованных в массиве дисков. В то же время такое решение не позволяет восстановить информацию при выходе из строя одного из дисков массива.

Среди всех вышеперечисленных уровней дисковых массивов уровни 3 и 5 являются наиболее предпочтительными и предполагают меньшие по сравнению с организацией "зеркальных" дисков материальные затраты при том же уровне надежности.

# 2. Характеристика физических средств защиты

**Физические средства защиты** - это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.

[](https://ru.bmstu.wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Tcoibl_11_3.png)

Физические средства защиты

К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий.

Эти средства применяются для решения следующих задач:

* охрана территории предприятия и наблюдение за ней;
* охрана зданий, внутренних помещений и контроль за ними;
* охрана оборудования, продукции, финансов и информации;
* осуществление контролируемого доступа в здания и помещение.

Все физические средства защиты объектов можно разделить на три категории:

1. средства предупреждения,
2. средства обнаружения
3. системы ликвидации угроз.

Охранная сигнализация и охранное телевидение, например, относятся к средствам обнаружения угроз; заборы вокруг объектов - это средства предупреждения несанкционированного проникновения на территорию, а усиленные двери, стены, потолки, решетки на окнах и другие меры служат защитой и от проникновения, и от других преступных действий (подслушивание, обстрел, бросание гранат и взрывпакетов и др.). Средства пожаротушения относятся к системам ликвидации угроз.

В общем плане по физической природе и функциональному назначению все средства этой категории можно разделить на следующие группы:

* охранные и охранно-пожарные системы;
* охранное телевидение;
* охранное освещение;
* средства физической защиты.

К средствам физической защиты относятся:

* ограждение и физическая изоляция,
* запирающие устройства,
* системы контроля доступа.

К системам контроля доступа относятся:

* системы, использующие различные карты и карточки, на которых помещается кодированная или открытая информация о владельце,
* системы опознавания по отпечаткам пальцев,
* системы опознавания по голосу,
* системы опознавания по почерку,
* система опознавания по геометрии рук.

Все устройства идентификации могут работать как отдельно, так и в комплексе.

Рекомендации по ограничению физического доступа к оборудованию связи.

Для достижения указанной цели следует применять аппаратуру, проверенную на отсутствие внедренных “закладок”, эксплуатируемую аппаратуру — пломбировать, ремонт аппаратуры производить только с привлечением доверенных специалистов под контролем владельца или сотрудника службы безопасности, исключить какие-либо инициативные переделки введенной в эксплуатацию аппаратуры обслуживающим персоналом или ремонтниками. Особое внимание следует обращать на легко заменяемые элементы. Например, кабель, соединяющий телефонный аппарат с аппаратом защиты (скремблером, шифратором) может быть заменен за несколько секунд, а его конструкция и габариты допускают установку весьма совершенной “закладки”. Такие элементы следует дополнительно закреплять и маркировать. Дополнительное крепление и маркировка должны быть незаметны для постороннего наблюдателя, но легко проверяться владельцем терминала или допущенным обслуживающим персоналом. Прокладка проводов, несущих сигналы незащищенной информации, должна выполняться скрыто, по возможности без разъемных соединений, функционально необходимые разъемы должны дополнительно фиксироваться или пломбироваться.

Отходящие цепи должны быть максимально удалены от аппаратуры обработки информации. Кабели, шнуры, несущие сигнала защищаемой информации, и находящиеся вблизи аппаратуры отходящие цепи должны быть экранированы.

В целом при организации рабочего места абонента защищенной связи следует придерживаться правил:

На рабочем месте должен быть минимум аппаратуры и оборудования; только то, что совершенно необходимо для рабочего процесса.

Установка всего оборудования и элементов интерьера должна предельно затруднять их перемещение и замену или внедрение посторонних предметов.

***Системы охраны периметров.***

Современные электронные системы охраны весьма разнообразны и в целом достаточно эффективны. Однако большинство из них имеют общий недостаток: они не могут обеспечить раннее детектирование вторжения на территорию объекта. Такие системы, как правило, ориентированы на обнаружение нарушителя, который уже проник на охраняемую территорию или в здание. Это касается, в частности, систем видеонаблюдения; они зачастую с помощью устройства видеозаписи могут лишь подтвердить факт вторжения после того, как он уже произошел.

Периметральная граница объекта является наилучшим местом для раннего детектирования вторжения, т.к. нарушитель взаимодействует в первую очередь с физическим периметром и создает возмущения, которые можно зарегистрировать специальными датчиками. Если периметр представляет собой ограждение в виде металлической решетки, то ее приходится перерезать или преодолевать сверху; если это стена или барьер, то через них нужно перелезть; если это стена или крыша здания, то их нужно разрушить; если это открытая территория, то ее нужно пересечь.

Датчик любой периметральной системы реагирует на появление нарушителя в зоне охраны или определенные действия нарушителя. Сигналы датчика анализируются электронным блоком (анализатором или процессором), который, в свою очередь, генерирует сигнал тревоги при превышении заданного порогового уровня активности в охраняемой зоне.

***Общие требования к периметральным системам.***

Любая периметральная система охраны должна отвечать определенному набору критериев, некоторые из которых перечислены ниже:

Возможность раннего обнаружения нарушителя — еще до его проникновения на объект

Точное следование контурам периметра, отсутствие “мертвых” зон

По возможности скрытая установка датчиков системы

Независимость параметров системы от сезона (зима, лето) и погодных условий (дождь, ветер, град и т.д.)

Невосприимчивость к внешним факторам “нетревожного” характера — индустриальные помехи, шум проходящего рядом транспорта, мелкие животные и птицы

Устойчивость к электромагнитным помехам — грозовые разряды, источники мощных электромагнитных излучений и т.п.

Очевидно, что периметральная охранная система должна обладать максимально высокой чувствительностью, чтобы обнаружить даже опытного нарушителя. В то же время эта система должна обеспечивать по возможности низкую вероятность ложных срабатываний. Причины ложных тревог могут быть различными. Система может, например, среагировать при появлении в зоне охраны птиц или мелких животных. Сигнал тревоги может появиться при сильном ветре, граде или дожде. Кроме того, ложная тревога может возникнуть из-за “технологических” причин: неграмотный монтаж датчиков на ограде, неправильная настройка электронных блоков или просто неудовлетворительное инженерное состояние самой ограды, которая может, например, вибрировать при сильном ветре.

Весьма важным фактором является квалификация и опыт организации, которая проектирует и монтирует периметральную систему охраны. Опыт показывает, что зачастую эффективность системы определяется не столько ее исходными техническими параметрами, сколько правильностью выбора и грамотностью ее монтажа.

Для оценки эффективности периметральных систем чаще всего используют специальные испытательные полигоны. Охранные системы там монтируют на стандартных оградах и оценивают их по специальным методикам, имитируя различные действия нарушителя — разрушение ограды, перелезание, подкоп и др.

**Специфика применения периметральных систем.**

Особенность периметральных систем состоит в том, что обычно они конструктивно интегрированы с ограждением и генерируемые охранной системой сигналы в сильной степени зависят как от физико-механических характеристик ограды (материал, высота, жесткость и др.), так и от правильности монтажа датчиков (выбор места крепления, метод крепления, исключение случайных вибраций ограды и т.п.). Очень большое значение имеет правильный выбор типа охранной системы, наиболее адекватно отвечающей данному типу ограды.

Периметральные системы используют, как правило, систему распределенных или дискретных датчиков, общая протяженность которых может составлять несколько километров. Такая система должна обеспечивать высокую надежность при широких вариациях окружающей температуры, при дожде, снеге, сильном ветре. Поэтому любая система должна обеспечивать соответствующую автоматическую адаптацию к погодным условиям и возможность дистанционной диагностики.

Любая периметральная система должна легко интегрироваться с другими охранными системами, в частности, с системой видеонаблюдения.

***Радиолучевые системы.***

Такие системы содержат приемник и передатчик СВЧ сигналов, которые формируют зону обнаружения в виде вытянутого эллипсоида вращения (рис.1). Длина отдельной зоны охраны определятся расстоянием между приемником и передатчиком, а диаметр зоны варьируется от долей метра до нескольких метров.

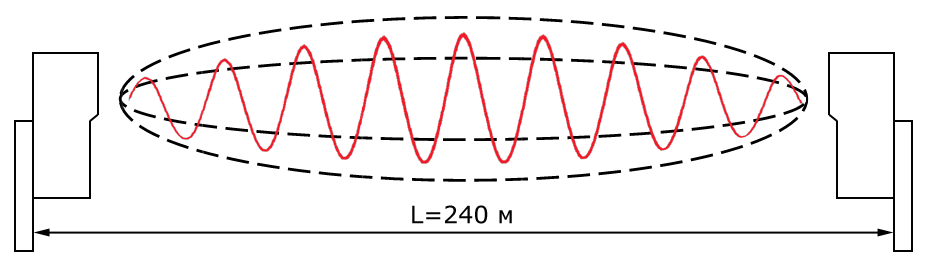
[](https://ru.bmstu.wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Tcoibl_15.png)

Рис. 1. Принцип действия радиолучевой системы.

Принцип действия таких систем основан на анализе изменений амплитуды и фазы принимаемого сигнала, возникающих при появлении в зоне постороннего предмета. Системы применимы там, где обеспечивается прямая видимость между приемником и передатчиком, т.е. профиль поверхности должен быть достаточно ровным и в зоне охраны должны отсутствовать кусты, крупные деревья и т.п.

Общим недостатком радиолучевых систем является наличие “мертвых” зон — чувствительность системы понижена вблизи приемника и передатчика, поэтому приемники и передатчики соседних зон должны устанавливаться с перекрытием в несколько метров. Кроме того, радиолучевые системы недостаточно чувствительны непосредственно над поверхностью земли (30 — 40 см), что может позволить нарушителю преодолеть рубеж охраны ползком.

Относительно широкая зона чувствительности системы обуславливает ограниченность ее применения на объектах, где возможно случайное попадание в зону обнаружения людей, транспорта и т.п. В таких ситуациях для предотвращения ложных срабатываний рекомендуется с помощью дополнительной ограды оборудовать предзонник.

***Радиоволновые системы.***

Чувствительным элементом такой системы является пара расположенных параллельно проводников (кабелей), к которым подключены соответственно передатчик и приемник радиосигналов. Вокруг проводящей пары (“открытой антенны”) образуется чувствительная зона, диаметр которой зависит от взаимного расположения проводников. При появлении человека в зоне чувствительности сигнал на выходе приемника изменяется и система генерирует сигнал тревоги.

При использовании радиоволновых систем на оградах, кабели устанавливают либо на специальных стойках на верхнем торце ограды, либо непосредственно на поверхности ограды.

Преимущества радиоволновых систем перед лучевыми — независимость от профиля почвы и точное следование линии ограды.

Одно из наиболее известных отечественных охранных устройств радиоволнового типа — система “Уран-М”— разработка предприятия НИКИРЭТ (г. Заречный, Пензенская обл.). Двухпроводная линия (рис. 2.) закрепляется на вертикальных или наклонных кронштейнах (консолях), выполненных из диэлектрика (входят в комплект поставки). В качестве проводников используется провод полевой телефонной связи П-274М, обеспечивающий достаточную механическую прочность и стойкость к атмосферным воздействиям. Длина одной зоны охраны находится в пределах от 10 до 250 м. Расстояние между соседними кронштейнами обычно составляет 6...8 м, в районах с сильными ветрами его рекомендуется уменьшать до 3...4 м.

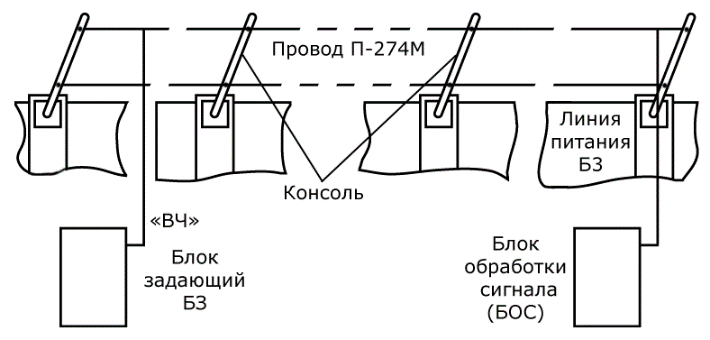
[](https://ru.bmstu.wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Tcoibl_16.png)

Рис. 2. Схема двухпроводного радиоволнового устройства.

Для протяженных периметров используют несколько комплектов “Уран-М”. Для исключения влияния соседних зон предусмотрен режим взаимной синхронизации до 22 — 25 отдельных комплектов. Радиоволновые системы можно устанавливать практически на любых жестких оградах (кирпич, бетон, металл).

Система настраивается для детектирования объекта массой более 30 — 40 кг и не срабатывает при попадании в зону птиц или мелких животных. Система не срабатывает при движении транспорта на расстоянии более 3 м от чувствительных проводников. Напряжение питания 20...30 В, ток питания — не более 100 мА. Обеспечен режим дистанционного контроля работоспособности. Охранное устройство устойчиво к воздействию сильного дождя (до 40 мм/час), снега, града и ветра со скоростью до 20 м/сек. Электронные блоки имеют размеры 255 х 165 х 110 мм, они сохраняют работоспособность в температурном диапазоне от -40О до +40О. Конструкция блоков обеспечивает защиту от внешних электромагнитных помех и высокой влажности.

# 3.Анализ технических средств обеспечения информационной безопасности

Вопросы технического обеспечения информационной безопасности предприятия решают не только ИТ-подразделения. В безопасном использовании информационных ресурсов заинтересовано руководство и другие службы компании.

Концепция защиты

Реализация стратегии защиты начинается с разработки Концепции информационной безопасности, которая включает:

принципы отнесения объектов инфраструктуры, программных, информационных и физических, к критичным, нуждающимся в повышенной защите;

основные принципы и способы защиты, механизмы выстраивания правил, по которым производится внедрение отдельных защитных элементов;

модель угроз, типовой профиль нарушителя безопасности;

требования к безопасности, сформированные по результатам аудита рисков;

все меры защиты, предполагаемые для реализации;

дополнительная к принятой в рамках действующего законодательства ответственность за соблюдение мер информационной безопасности и утечку данных.

Концепция принимается на уровне высшего руководства предприятия и должна пересматриваться по мере эволюции информационной инфраструктуры и изменения модели угроз. На первом этапе для ее разработки собираются мнения всех подразделений, заинтересованных в системном решении задачи технического обеспечения информационной безопасности. В дальнейшем задача ее доработки по итогам контроля работоспособности может быть возложена на курирующее ИТ-подразделение.

Объекты защиты

Неожиданным для сотрудников ИТ-подразделений, но важным для экономической безопасности предприятия становится такой объект защиты, как вложенные в создание технической инфраструктуры инвестиции. Их окупаемость должна стать одной из важных задач предприятия, недопустима избыточность, при которой ИБ становится самоцелью, отнимая ресурсы у бизнес-процессов.

Экономический эффект от внедрения системы технической защиты конфиденциальных данных проявляется в:

доступности информации, когда ИТ-инфраструктура предприятия позволяет в любое время получить необходимые сведения. Пример несоответствия инфраструктуры критериям доступности – сайт Росреестра, информацию с которого иногда не могут получить даже Служба судебных приставов и Правительство Москвы, что привлекло внимание Контрольного управления Администрации Президента;

в целостности данных, отсутствии сбоев или постороннего вмешательства в их структуру, вызвавших искажение сведений, которое может привести к некорректности, принимаемых решений на их основе. В том же Росреестре на запрос выписки по объекту недвижимости в Рязани из-за сбоев в системе клиент может получить сведения о квартире в Уфе;

конфиденциальности информации. Соблюдение этого требования поможет избежать убытков от хищения конфиденциальной информации и штрафов в результате нарушения требований законодательства о персональных данных;

отсутствии возможностей отказаться от совершенной операции, это важно, например, при использовании онлайн-платежей;

аутентичности или полноценной системе подтверждения подлинности информации или электронных сообщений.

Традиционно объектами защиты становятся:

узлы ИС (серверы, рабочие станции);

технические средства, маршрутизаторы;

каналы связи, протоколы удаленного доступа;

программные средства, вне зависимости от того, разработаны они самостоятельно или сторонними разработчиками;

базы данных, собственные и находящиеся в облаке;

методы защиты данных.

Часто объекты разнесены в пространстве, на промышленных предприятиях многие из них могут находиться в труднодоступных местах. Каждый объект защиты должен быть описан в концепции обеспечения безопасности с учетом его относительной ценности и возможности замены.

Классификация пользователей

Часто выбор технического обеспечения информационной безопасности предприятия зависит от типов пользователя и количества групп пользователей на предприятии. В общем значении под пользователем подразумевается сотрудник, идентифицируемый в системе под собственным логином и паролем и имеющий доступ к данным в соответствии со своими служебными обязанностями. Технические и программные средства защиты информации должны давать возможность не только идентифицировать пользователей, но и разграничивать их доступ к данным разной категории.

В обычной компании достаточно выделить лица с правами пользователей и с правами администраторов. На производственном предприятии выделяют следующие группы пользователей:

руководство;

инженеры и разработчики;

наладчики оборудования;

персонал, обслуживающий оборудование, в том числе движущиеся объекты;

офисный персонал;

сотрудники компаний-аутсорсеров.

Для всех необходимо установить правила допуска, а также регламент их изменения. Права предоставляются по принципу минимально необходимых для решения служебных задач. Наиболее простое решение – открыть доступ пользователям к ресурсам исходя из типа программных модулей. К специализированным модулям относятся АСУ, банковские программы, системы управления безопасностью, к общедоступным – программы электронного документооборота (ЭДО), CRM-системы, корпоративная электронная почта.

Группа администраторов в ИТ-подразделении также не едина, в зависимости от сложности задач, стоящих перед службой, внутри нее могут выделяться отделы:

развития и технической эксплуатации ИС;

информационной безопасности;

мониторинга угроз и инцидентов;

технической поддержки пользователей;

информационно-аналитический.

Также в отдельную группу выделяют сотрудников филиалов и удаленных рабочих мест.

Функционал каждого подразделения в части технического обеспечения информационной безопасности предприятия прописывается в общем положении и должностных инструкциях сотрудников.

Корпоративная сеть предприятия

ИС выступает самостоятельным объектом защиты, так как необходимо обеспечить ее целостность на основе сетевого протокола TCP/IP.

При формировании архитектуры выделяются адресные пространства:

выделенные филиалам и обособленным подразделениям;

выделенные аппарату управления компании;

для адресации магистрального сегмента корпоративной сети;

резервное.

В рамках внешних потоков информации, подлежащих особенной защите, выделяют:

взаимодействие с банками по системе платежей Банк-Клиент;

передача бухгалтерской, налоговой, статистической отчетности в ФНС и внебюджетные фонды;

торговые трансакции при проведении сделок по продаже товаров или услуг в Интернете;

взаимодействие с клиентами по электронной почте;

взаимодействие по Интернету с биржами и торговыми площадками для участия в тендерах или закупках;

направление отчетной информации в проверяющие организации.

Эти виды коммуникации содержат большие объемы конфиденциальной информации, которую необходимо защищать от утечек.

Взаимодействие организуется по трем каналам:

выделенный магистральный канал сообщения с корпоративной сетью с использованием протоколов VPN, скрывающих трафик;

резервная линия связи с Интернетом;

коммутируемый канал связи посредством использования технологии GPRS.

Совмещение этих трех защищенных каналов позволяет уберечь информацию, представляющую наибольший интерес для злоумышленников. Из средств технического обеспечения информационной безопасности предприятия дополнительно используются магистральные роутеры и межсетевые экраны. Задача регламентированного подключения пользователей к Интернету решается на основе системных политик компании.

Факторы, учитываемые при разработке стратегии ИБ

Меняющаяся реальность и увеличивающийся объем угроз побуждают организации постоянно видоизменять концепцию защиты информационных активов.

# Заключение

Следует отметить, что при всей кажущейся простоте предлагаемых мер, их реализация и, главное, оценка эффективности требует глубокого анализа конкретной аппаратуры связи, ее размещения и помещения, в котором установлен терминал. Это связано с тем, что большинство процессов, приводящих к утечке информации (за исключением непосредственного подключения злоумышленника к линии связи) носит паразитный характер, не нормируется документацией на аппаратуру, не проявляется в основном рабочем процессе. Многие параметры этих процессов существенно изменяются от экземпляра к экземпляру аппаратуры связи и сопряженных с ней изделий, существенно зависят от воздействий, не влияющих на основной рабочий процесс (например, от перемещения кабелей питания). Оценка значимости тех или иных паразитных процессов в конкретной ситуации, выбор рациональных мер их подавления, формирование правил эксплуатации терминала в части поддержания на требуемом уровне его информационной защищенности требуют высокой квалификации и качественно могут быть выполнены только с привлечением специализированной организации.

Техническое обеспечение информационной безопасности предприятия после его внедрения призвано решить следующие задачи:

защита периметра сетей от несанкционированных внешних вторжений и подключений. В этих целях применяются маршрутизаторы, брандмауэры, контроль удаленного доступа;

защита серверов компании от НСД, как внешнего, так и инсайдерского, за счет внедрения систем аутентификации и модели дифференцированного доступа;

комплексная антивирусная защита, при реализации которой решается задача защиты серверов, рабочих станций пользователей, внешнего шлюза, соединяющего с Интернетом;

организация системы мониторинга уязвимостей и реакции на них, мгновенно оповещающей системных администраторов об угрозах. ПО, используемое для мониторинга, должно обновляться таким образом, чтобы выявлять новые угрозы;

защита приложений и сервисов, устранение угрозы их сбоя и остановки реализации бизнес-процессов;

защита межсетевых взаимодействий, выделение отдельных зон для запуска значимых процессов.

Аудит должен проверить выполнение всех требований и подготовить доклад с рекомендациями по дальнейшему улучшению системы.

Организационные, технические и программные средства защиты

Для любой компании реализация системы технической безопасности инфраструктуры начинается с принятия пакета прикладных организационных мер. Основным документом окажется Политика информационной безопасности, многие внутренние регламенты могут быть разработаны в качестве приложений к ней. Не рекомендуется оформлять в качестве приложений документы, разработка которых регламентирована необходимостью защиты персональных данных и выполнений требований регулятора.

Персонал должен быть ознакомлен с документами. Они должны храниться в доступном для ознакомления месте, например, на сервере компании.

Если реализация мероприятий по созданию системы технического обеспечения информационной безопасности предприятия осуществляется организацией-подрядчиком, она должна иметь лицензии. Выполнение комплекса мер позволит обеспечить защиту интересов фирмы на высшем уровне

# Список литературы

1. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ, 2016. — 239 c.
2. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2017. — 536 c.
3. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 c.
4. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 c.
5. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2016. — 432 c.
6. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА, 2016. — 296 c.