Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты

Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты

Преподаватель: Сидиков И.Д.

Общие принципы обеспечения безопасности объектов

В общем случае обеспечение безопасности объекта базируется на двух принципах:

1. Определение и оценка угроз объекту;
2. Разработка и реализация адекватных мер защиты.

Адекватные меры защиты предусматривают:

1. Тотальный контроль несанкционированного проникновения на территорию объекта, в здания и помещения;
2. Ограничение и контроль доступа людей в «закрытые» здания и помещения с возможностью документирования результатов контроля;
3. Обнаружение злоумышленника на самых ранних этапах его продвижения к цели акции;
4. Оценку ситуации;
5. Создание на пути продвижения нарушителя физических препятствий, обеспечивающих задержку, необходимую силам охраны для его перехвата;
6. Принятие немедленных действий по развертыванию сил охраны и пресечению действий злоумышленников;
7. Видеодокументирование действий персонала на особо ответственных участках объекта.

Lifecycle Security

Роль анализа рисков для создания корпоративной системы защиты информации в компьютерной сети предприятия можно наглядно показать на примере модели Lifecycle Security (название можно перевести как "жизненный цикл безопасности"), разработанной компанией Axent, впоследствии приобретенной Symantec.

Lifecycle Security - это обобщенная схема построения комплексной защиты компьютерной сети предприятия. Выполнение описываемого в ней набора процедур позволяет системно решать задачи, связанные с защитой информации, и дает возможность оценить эффект от затраченных средств и ресурсов. С этой точки зрения, идеология Lifecycle Security может быть противопоставлена тактике "точечных решений", заключающейся в том, что все усилия сосредотачиваются на внедрении отдельных частных решений (например, межсетевых экранов или систем аутентификации пользователей по смарт-картам). Без предварительного анализа и планирования, подобная тактика может привести к появлению в компьютерной системе набора разрозненных продуктов, которые не стыкуются друг с другом и не позволяют решить проблемы предприятия в сфере информационной безопасности.

Компоненты модели LifeCycle Security

Политики безопасности, стандарты, процедуры и метрики. Этот компонент определяет рамки, в которых осуществляются мероприятия по обеспечению безопасности информации, и задает критерии оценки полученных результатов. Стоит отметить, что под стандартами здесь понимаются не только государственные и международные стандарты в сфере информационной безопасности, но и корпоративные стандарты, которые в ряде случаев могут оказать очень существенное влияние на создаваемую систему защиты информации. Также хочется остановиться на обязательном введении метрики, позволяющей оценить состояние системы до и после проведения работ по защите информации. Метрика определяет, в чем и как измеряем защищенность системы, и позволяет соотнести сделанные затраты и полученный эффект.

Анализ рисков. Этот этап является отправной точкой для установления и поддержания эффективного управления системой защиты. Проведение анализа рисков позволяет подробно описать состав и структуру информационной системы (если по каким-то причинам это не было сделано ранее), расположить имеющиеся ресурсы по приоритетам, основываясь на степени их важности для нормальной работы предприятия, оценить угрозы и идентифицировать уязвимости системы.

Компоненты модели LifeCycle Security

Стратегический план построения системы защиты. Результаты анализа рисков используются как основа для разработки стратегического плана построения системы защиты. Наличие подобного плана помогает распределить по приоритетам бюджеты и ресурсы, и в последующем осуществить выбор продуктов и разработать стратегию их внедрения.

Выбор и внедрение решений. Хорошо структурированные критерии выбора решений в сфере защиты информации и наличие программы внедрения уменьшает вероятность приобретения продуктов, становящихся "мертвым грузом", мешающим развитию информационной системы предприятия. Кроме непосредственно выбора решений, также должно учитываться качество предоставляемых поставщиками сервисных и обучающих услуг. Кроме того, необходимо четко определить роль внедряемого решения в выполнении разработанных планов и достижении поставленных целей в сфере безопасности.

Обучение персонала. Знания в области компьютерной безопасности и технические тренинги необходимы для построения и обслуживания безопасной вычислительной среды. Усилия, затраченные на обучение персонала, значительно повышают шансы на успех мероприятий по защите сети.

Компоненты модели LifeCycle Security

Мониторинг защиты. Он помогает обнаруживать аномалии или вторжения в ваши компьютеры и сети и является средством контроля над системой защиты, чтобы гарантировать эффективность программ защиты информации.

Разработка методов реагирования в случае инцидентов и восстановление. Без наличия заранее разработанных и "отрепетированных" процедур реагирования на инциденты в сфере безопасности невозможно гарантировать, что в случае обнаружения атаки ей будут противопоставлены эффективные меры защиты, и работоспособность системы будет быстро восстановлена.

Все компоненты программы взаимосвязаны и предполагается, что процесс совершенствования системы защиты идет непрерывно.

Этап анализов рисков

По мнению разработчиков модели Lifecycle Security, он должен проводиться в следующих случаях:

- До и после обновления или существенных изменений в структуре системы;
- До и после перехода на новые технологии;
- До и после подключения к новым сетям (например, подключения локальной сети филиала к сети головного офиса);
- До и после подключения к глобальным сетям (в первую очередь, интернет);
- До и после изменений в порядке ведения бизнеса (например, при открытии электронного магазина);
- Периодически, для проверки эффективности системы защиты.

Ключевые моменты этапа анализа рисков:

- Подробное документирование компьютерной системы предприятия. При этом особое внимание необходимо уделять критически важным приложениям.
- Определение степени зависимости организации от нормального функционирования фрагментов компьютерной сети, конкретных узлов, от безопасности хранимых и обрабатываемых данных.
- Определение уязвимых мест компьютерной системы.
- Определение угроз, которые могут быть реализованы в отношении выявленных уязвимых мест.
- Определение и оценка всех рисков, связанных с эксплуатацией компьютерной системы.

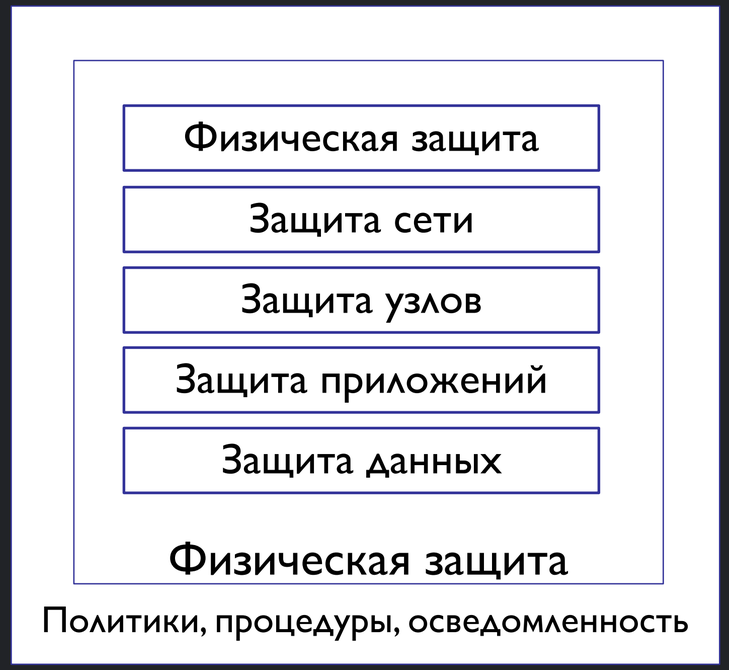
Этап анализов рисков

Особо хочется обратить внимание на связь анализа рисков с другими компонентами модели. С одной стороны, наличие метрики защищенности и определение значений, характеризующих состояние системы до и после мероприятий по защите информации, накладывает определенные требования на процедуру анализа рисков. Ведь на базе полученных результатов и оценивается состояние системы. С другой стороны, они дают те начальные условия, исходя из которых, разрабатывается план построения системы защиты сети. И результаты анализа рисков должны быть сформулированы в виде, пригодном для выполнения как первой, так и второй функции.

Модель многоуровневой защиты

Понятие многоуровневой защиты или эшелонированной обороны, а в английской версии - Defence (амер. Defense) in depth, пришло в информационные технологии из военных руководств.

С точки зрения информационной безопасности, модель многоуровневой защиты определяет набор уровней защиты информационной системы. Модель часто используется корпорацией Майкрософт в руководствах по безопасности. Корректная организация защиты на каждом из выделенных уровней, позволяет уберечь систему от реализации угроз информационной безопасности.



Модель многоуровневой защиты

Политика безопасности должна описывать все аспекты работы системы с точки зрения обеспечения информационной безопасности. Поэтому уровень политики безопасности можно рассматривать как базовый. Этот уровень также подразумевает наличие документированных организационных мер защиты (процедур) и порядка информирования о происшествиях, обучение пользователей в области информационной безопасности и прочие меры аналогичного характера (например, рекомендуемые стандартом ISO/IEC 17799).

Уровень физической защиты включает меры по ограничению физического доступа к ресурсам системы - защита помещений, контроль доступа, видеонаблюдение и т.д. Сюда же относятся средства защиты мобильных устройств, используемых сотрудниками в служебных целях.

Уровень защиты периметра определяет меры безопасности в "точках входа" в защищаемую сеть из внешних, потенциально опасных. Классическим средством защиты периметра является межсетевой экран (англ. термин - firewall), который на основании заданных правил определяет, может ли проходящий сетевой пакет быть пропущен в защищаемую сеть. Другие примеры средств защиты периметра - системы обнаружения вторжений, средства антивирусной защиты для шлюзов безопасности и т.д.

Модель многоуровневой защиты

Уровень защиты внутренней сети "отвечает" за обеспечение безопасности передаваемого внутри сети трафика и сетевой инфраструктуры. Примеры средств и механизмов защиты на этом уровне - создание виртуальных локальных сетей (VLAN) с помощью управляемых коммутаторов, защита передаваемых данных с помощью протокола IPSec и т.д. Нередко внутри сети также используют средства, характерные для защиты периметра, например, межсетевые экраны, в том числе и персональные (устанавливаемые на защищаемый компьютер).
Связано это с тем, что использование беспроводных сетевых технологий и виртуальных частных сетей (VPN) приводит к "размыванию" периметра сети.
Например, если атакующий смог подключиться к точке беспроводного доступа внутри защищаемой сети, его действия уже не будут контролироваться межсетевым экраном, установленным "на границе" сети, хотя формально атака будет производиться с внешнего по отношению к нашей сети компьютера. Поэтому иногда при анализе рассматривают "уровень защиты сети", включающий и защиту периметра, и внутренней сети.

Модель многоуровневой защиты

Следующим на схеме идет уровень защиты узлов. Здесь рассматриваются атаки на отдельный узел сети и, соответственно, меры защиты от них. Может учитываться функциональность узла и отдельно рассматриваться защита серверов и рабочих станций. В первую очередь, необходимо уделять внимание защите на уровне операционной системы - настройкам, повышающим безопасность конфигурации (в том числе, отключению не использующихся или потенциально опасных служб), организации установки исправлений и обновлений, надежной аутентификации пользователей. Исключительно важную роль играет антивирусная защита.

Уровень защиты приложений отвечает за защиту от атак, направленных на конкретные приложения - почтовые серверы, web-серверы, серверы баз данных. В качестве примера можно назвать SQL-инъекции - атаки на сервер БД, заключающиеся в том, что во входную текстовую строку включаются операторы языка SQL, что может нарушить логику обработки данных и привести к получению нарушителем конфиденциальной информации. Сюда же можно отнести модификацию приложений компьютерными вирусами. Для защиты от подобных атак используются настройки безопасности самих приложений, установка обновлений, средства антивирусной защиты.

Модель многоуровневой защиты

Уровень защиты данных определяет порядок защиты обрабатывающихся и хранящихся в системе данных от несанкционированного доступа и других угроз. В качестве примеров контрмер можно назвать разграничение доступа к данным средствами файловой системы, шифрование данных при хранении и передаче.

В процессе идентификации рисков определяется, что является целью нарушителя, и на каком уровне или уровнях защиты можно ему противостоять. Соответственно выбираются и контрмеры. Защита от угрозы на нескольких уровнях снижает вероятность ее реализации, а значит, и уровень риска.

Методика управления рисками, предлагаемая Microsoft

Управление рисками рассматривается как одна из составляющих общей программы управления, предназначенной для руководства компаний и позволяющей контролировать ведение бизнеса и принимать обоснованные решения

Процесс управления рисками безопасности, предлагаемый Майкрософт, включает следующие четыре этапа:

1. Оценка рисков
- Планирование сбора данных. Обсуждение основных условий успешной реализации и подготовка рекомендаций.
- Сбор данных о рисках. Описание процесса сбора и анализа данных.
- Приоритизация рисков. Подробное описание шагов по качественной и количественной оценке рисков.

Методика управления рисками, предлагаемая Microsoft

2. Поддержка принятия решений

- Определение функциональных требований. Определение функциональных требований для снижения рисков.
- Выбор возможных решений для контроля. Описание подхода к выбору решений по нейтрализации риска.
- Экспертиза решения. Проверка предложенных элементов контроля на соответствие функциональным требованиям.
- Оценка снижения риска. Оценка снижения подверженности воздействию или вероятности рисков.
- Оценка стоимости решения. Оценка прямых и косвенных затрат, связанных с решениями по нейтрализации риска.
- Выбор стратегии нейтрализации риска. Определение наиболее экономически эффективного решения по нейтрализации риска путем анализа выгод и затрат.

Методика управления рисками, предлагаемая Microsoft

3. Реализация контроля. Развертывание и использование решений для контроля, снижающих риск для организации.
   - Поиск целостного подхода. Включение персонала, процессов и технологий в решение по нейтрализации риска.
   - Организация по принципу многоуровневой защиты. Упорядочение решений по нейтрализации риска в рамках предприятия.

4. Оценка эффективности программы. Анализ эффективности процесса управления рисками и проверка того, обеспечивают ли элементы контроля надлежащий уровень безопасности.
   - Разработка системы показателей рисков. Оценка уровня и изменения риска.
   - Оценка эффективности программы. Оценка программы управления рисками для выявления возможностей усовершенствования.

Интегрированные системы безопасности - принципы построения и возможности

Бурное развитие современных технических средств безопасности и расширение выполняемых ими функций позволяет эффективно противодействовать внешним угрозам. В то же время усложняется процесс управления, увеличивается число управляющих устройств и, как следствие, растет нагрузка на службу безопасности. Сегодня решение всего комплекса задач по обеспечению безопасности объекта подразумевает наличие значительного объема работы по учету, контролю и статистической обработке информации. Часть наиболее трудоемких функций в этой области можно и нужно передать электронной системе безопасности.

Безопасность объекта, как правило, обеспечивается несколькими системами: охранной и пожарной сигнализации (ОПС), теленаблюдения (CCTV) и системой контроля управления доступом (СКУД). В этот "классический" набор также могут входить: система периметральной охраны, активного пожаротушения, инженерно-технические подсистемы обеспечения жизнедеятельности здания и др.

Интегрированные системы безопасности - принципы построения и возможности

Каждая из этих систем в отдельности отвечает за свой участок работы в соответствии с решаемыми задачами, заложенными в нее на этапе проектирования. К сожалению, вследствие их узкой направленности могут возникать противоречия при решении конкретных ситуаций на объекте, приводящие к серьезным проблемам:

- Потере эффективности и оперативности действий службы безопасности, перегруженной большим количеством "разнокалиберных" управляющих терминалов;
- Усложнению специализированных устройств управления в связи с появлением новых функций;
- Несогласованности в работе различных подсистем;
- Возможной выдаче подсистемами взаимоисключающих команд.

Возникает необходимость взаимодействия отдельных подсистем в рамках единой интегрированной системы безопасности (ИСБ).

Интегрированные системы безопасности - принципы построения и возможности

Современные ИСБ представляют собой аппаратно-программные комплексы с общей базой данных - единым информационным полем. В качестве устройств управления используются компьютерные терминалы со специализированным программным обеспечением.

Благодаря слиянию отдельных подсистем и применению компьютера в качестве универсального устройства управления достигается:

- Автоматизация простейших действий и реакций на внешние события – рутинную работу берет на себя электроника, обеспечивающая мгновенную реакцию на возникшее событие;
- Снижение влияния человеческого фактора на надежность системы;
- Взаимодействие аппаратуры разного назначения, исключающее противоречивые команды благодаря гибкой системе внутренних приоритетов;
- Упрощение процесса управления;
- Разграничение прав и доступа к информации;
- Повышение степени защиты от несанкционированного доступа к управлению;
- Общее снижение затрат за счет исключения дублирующей аппаратуры;
- Повышение степени эффективности каждой из подсистем и пр.

Интегрированные системы безопасности - принципы построения и возможности

В качестве базовых функций современных ИСБ можно указать следующие:

- Разграничение полномочий, регистрация и документирование проходов персонала в служебные помещения;
- Раздельная постановка и снятие с охраны каждой зоны или группы зон (в том
- Числе и автоматически по чтению электронной карты);
- Дистанционный видеоконтроль и видеорегистрация с сохранением базы данных
- Видеофрагментов;
- Документирование всех событий в системах с возможностью оперативного
- Получения различных отчетов по заданным параметрам фильтрации (как в СКУД, так и в ОПС);
- Документирование действий персонала с целью предупреждения актов
- Саботажа;
- Возможность оперативного вмешательства в работу системы;
- Возможность управления инженерными коммуникациями;
- Сохранение основного функционала каждой из подсистем при нарушении связи
- Между ними.

Способы интеграции

В реальных системах наиболее распространены три типа интеграции: на уровне "сухих контактов", на системном уровне и смешанный тип.

Первый вид интеграции – наиболее простой распространен в небольших системах. Фактически это интеграция на физическом уровне, при которой релейные выходы какой-либо из подсистем (например, ОПС), связываются со входами другой подсистемы (например, теленаблюдения).
Принцип прост: сработало реле (по команде охранного датчика), включилось устройство (мультиплексор включил телекамеру).

Способы интеграции

Интеграция на программном уровне обычно подразумевает возможность управления подсистемами ИСБ с помощью команд с компьютерного терминала, используя какой-либо коммуникационный протокол (например, RS-232 или RS-485). Имея единую базу данных, а также гибкий универсальный инструмент управления в виде компьютера и программного обеспечения, можно задавать сложные иерархические связи между подсистемами безопасности. Данный тип интеграции позволяет использовать в одной системе оборудование не только разного назначения, но и различных производителей. Этим достигается повышенная гибкость при конфигурировании конкретной ИСБ, адекватность затрат и угроз.

Недостатком метода является его уязвимость из-за программного механизма интеграции, а достоинством – гибкость, возможность конфигурирования сложных крупных систем и интеграция в ИСБ уже установленного на объекте оборудования. На крупных и распределенных объектах обычно используют данный тип интеграции, снижая недостатки за счет использования подсистем с возможностью автономной работы и применяя для некоторых из подсистем глубокую аппаратную интеграцию на уровне протокола.

Способы интеграции

Аппаратная интеграция на уровне протокола обычно используется в различных подсистемах ИСБ одного производителя (поскольку требуется глубокое знание аппаратной части и протокола обмена оборудования на уровне разработчика системы). Обычно это характерно для подсистем СКУД и ОПС, логика работы которых сильно взаимосвязана. При этом охраняются внутренние логические связи подсистем и их функции даже в случае отключения компьютера, но отсутствует гибкость, появляется привязка к одному производителю и невозможность интеграции оборудования сторонних компаний.
Надо также отметить, что вероятность наличия в производственной линейке данного производителя всех требуемых на объекте подсистем довольно низка (нельзя предусмотреть все).

Для интеграции смешанного типа характерно применение в менее значимых местах интеграции на уровне "сухих контактов"; для подсистем, требующих глубокого уровня взаимодействия, – интеграция на уровне протокола и работа с подсистемами сторонних производителей с использованием программной интеграции.

СКУД и охранная сигнализация

Как правило, СКУД выполняет в ИСБ главенствующую роль, поскольку обладает наиболее мощной и развитой встроенной логикой. Данная подсистема непосредственно связана с компьютерными терминалами управления. Наиболее важные функции СКУД:

- Управление процессом доступа в соответствии с заранее присвоенными
- Полномочиями;
- Регистрация факта прохода с привязкой ко времени;
- Возможность управления процессом доступа в отдельные помещения;
- Автоматизация действий и реакций.

Применение электронных СКУД не исключает участие человека в процессе управления. Охранная сигнализация наиболее часто интегрируется с СКУД на уровне протокола (самом глубоком уровне), поскольку охрана помещений тесно связана с правом прохода в них людей.
Наиболее типичный пример подобной интеграции – снятие с охраны помещения при проходе в него человека с соответствующими полномочиями.

СКУД и охранная сигнализация

Пример:

Подсистема СКУД зарегистрировала факт нарушения сотрудником Ивановым времени прохода в помещение бухгалтерии, после которого обнаружилась пропажа важных документов. Факт несанкционированного прохода был также задокументирован системой теленаблюдения, получившей сигнал от СКУД. Подтверждение разрешения на проход поступило от дежурного оператора ИСБ. В итоге на рабочем месте Иванова обнаружены пропавшие документы, и он уволен. Дежурный оператор службы безопасности получил строгий выговор с понижением полномочий в управлении системой.

Интеграция с системой теленаблюдения (CCTV)

В ИСБ подсистема теленаблюдения существенно повышает свою эффективность, поскольку становится возможным активирование камер теленаблюдения по событиям в подсистемах СКУД и ОПС.

Пример:

Сработала система пожарной сигнализации. На управляющий монитор автоматически выводится план объекта с указанием сработавшего пожарного датчика. одновременно подается звуковой сигнал тревоги и команда на запись изображения с ближайшей камеры с одновременным выводом данного изображения на монитор. В случае отсутствия команды со стороны оператора в течении нескольких секунд (заснул, отошел и т.д.) ИСБ автоматически выдает команду подсистеме СКУД на разблокирование всех дверей по пути эвакуации из указанного помещения.

Фактически в ИСБ охранник может обслужить значительно большее количество камер.

Интеграция с системой теленаблюдения (CCTV)

Простейший пример интеграции CCTV со СКУД – режим "спецконтроль", при котором чтение карты на считывателе СКУД сопровождается выводом на компьютер фотографии человека из базы данных с одновременной выдачей изображения с телекамеры. Охранник сличает два изображения и принимает решение о праве доступа. Следует отметить все возрастающее значение и число цифровых CCTV с записью изображения на жесткий ный цифровой видеорегистратор. В ИСБ применение цифровых CCTV позволяет реализовать новые полезные для службы безопасности функции, например:

- Быстрый доступ к архиву видеофрагментов и привязка его к событиям в ИСБ;
- Удобство хранения;
- Работа с видеосервером по сети.

Программное обеспечение

Программное обеспечение является важнейшей частью ИСБ. Общие требования к нему таковы:

- Удобный, графический интерфейс с планами объекта;
- Возможность управления как отдельными объектами, так и всей системой;
- Протоколирование событий (тревог, проходов в помещения и пр.) И действий
- Оператора в памяти компьютера;
- Парольная защита прав доступа операторов;
- Редактирование базы данных карт, запись в нее данных пользователя;
- Автоматизация формирования списка сообщений системы для просмотра,
- Распечатки и анализа;
- Учет рабочего времени;
- Программирование реакций системы на внешние события.

Программное обеспечение

Предпочтительным является использование отечественного программного обеспечения, поскольку его доработка под конкретные требования для зарубежных продуктов маловероятна.
Современный программный комплекс (ПК) для управления ИСБ должен быть гибкой, настраиваемой, масштабируемой системой.

Наиболее перспективными являются ПК, имеющие модульную структуру и мультиплатформенную архитектуру.

Модульность, прежде всего, позволяет стандартизировать процесс разработки новых драйверов и упрощает их интеграцию в существующий ПК.

Мультиплатформенность, в свою очередь, позволяет системе функционировать на самых разных аппаратно-программных платформах.

В наиболее "продвинутых" системах при выходе из строя или выключении отдельных узлов сети ранее выполняемые ими функции либо переносятся на другой узел, либо временно отключаются, но функционирование всей системы в целом не нарушается.

Дополнительным "козырем" может стать открытость ПК для сторонних разработчиков, когда заказчику предоставляется возможность разработки собственных драйверов оборудования.

Автономная работа

Поскольку компьютер является наиболее уязвимой частью ИСБ, важным элементом ее функционирования является возможность работы подсистем в автономном режиме с сохранением основных функций. Поскольку многие современные ИСБ строятся на основе аппаратуры СКУД, целесообразным представляется программирование наиболее важных действий системы на уровне контроллера СКУД.

Важным аспектом живучести ИСБ является возможность полностью автономной работы каждой из подсистем при серьезных повреждениях управляющего центра. В связи с этим целесообразно иметь минимально необходимое количество аппаратных терминалов управления подсистемами, обеспечивающих функции управления до момента восстановления главного управляющего центра.

Ключевые возможности ИСБ

Централизованное управление всем комплексом систем безопасности, возможность дистанционного мониторинга позволяют оператору составить максимально полную картину функционирования объекта и состояния его подсистем, что дает возможность принять правильное решение.

Тесное взаимодействие подсистем

В современной ИСБ можно запрограммировать логику работы системы с учетом сложных комбинаций сигналов от различных подсистем. За счет этого можно добиться существенного сокращения времени реакции на события, предоставив право решения в конкретных случаях электронике, а также снижения влияния человеческого фактора за счет автоматизации действий и реакций.

Протоколирование событий

Регистрация и документирование всех действий оператора и работы отдельных подсистем позволяет совершенствовать работу ИСБ, а также обеспечивает необходимым рабочим материалом должностных лиц, ответственных за безопасность объекта. На основе анализа данных материалов можно реально оценить правильность работы персонала, установить факты противоправных действий, зарегистрировать тревоги и факты несанкционированного доступа.

Пример:

Сработала система охранной сигнализации. На управляющем мониторе выводится план объекта с указанием конкретного охранного датчика, который выдал сигнал. Оператор (на том же мониторе) выводит изображение от ближайшей камеры теленаблюдения и визуально контролирует ситуацию. В случае ложного срабатывания тревога отменяется. Получаем адекватную реакцию на тревожную ситуацию. Необходимо провести диагностику датчика и в случае неисправности заменить его.

Особенности инженерно-технической защиты информации

Инженерно-техническая защита (ИТЗ) – это совокупность технических средств и мероприятий, нацеленных на предотвращение утечек, разглашения информации, и несанкционированного доступа в сетевые ресурсы организации. Актуальность защиты информации обусловливается наличием большого числа потенциальных конкурентов, а также недоброжелателей, которые могут навредить компании. Попав в чужие руки, ценная информация становится товаром. Ее искажение, порча или плагиат могут навредить репутации и финансам компании, причинить вред и способствовать выходу с рынка.

Защита конфиденциальности информации для многих предприятий стала первостепенной задачей, от качества решения которой зависит конкурентоспособность и возможность успешно выводить на рынок технологические новинки. Используя современные инженерно-технические средства можно обеспечить защиту сведений, относящихся к категории секретных или конфиденциальных.

Особенности инженерно-технической защиты информации

Чем вызвана необходимость в инженерно-технической защите информации?

1. Активным развитием средств добычи информации, которые, в том числе, позволяют получать несанкционированный доступ к данным на расстоянии.
2. Оснащением жилых, производственных и служебных помещений радио- и электроаппаратурой, неполадки в работе которых нередко способствуют утечке конфиденциальной информации.
3. Достижениями микроэлектроники (аудиожучки, миникамеры), которые стали доступны обычным пользователям и могут быть использованы для нелегальной добычи информации из скрытых источников.

Использование надежных технических средств защиты информации становится единственным способом предотвратить утечку данных. Именно поэтому будет полезным узнать, какие методы защиты информации являются наиболее надежными и целесообразными в применении.

Основные виды инженерно-технической защиты информации

Существует классификация инженерно-технической защиты информации по виду, объектам воздействия и используемым технологиям. Выделяют следующие виды средств инженерно-технической защиты:

- Физические. Используются с целью решения задач по охране предприятия, наблюдению за территорией и помещениями, осуществлению контролируемого доступа в здание. К ним относят охранно-пожарные системы, аварийное и локальное освещение, а также охранное телевидение. Физические средства защиты информации можно разделить на предупредительные, обнаруживающие и ликвидирующие угрозы, активно используемые сегодня руководителями многих предприятий.
- Аппаратные. К ним относятся электронные и механические устройства, предназначенные для инженерно-технической защиты информации и для противодействия шпионажу. Их главная задача – выявление каналов утечки информации, их локализация (обнаружение) и нейтрализация. Примерами таких средств могут служить комплексы для поиска сетевых радиопередатчиков, телефонных закладок и радиомикрофонов, устанавливаемых с целью секретного прослушивания.

Основные виды инженерно-технической защиты информации

- Программные. Включают в себя системы по защите информации, обеспечивающие защиту секретных данных: проектов, чертежей, стратегических и тактических задач фирмы, финансовых и бухгалтерских данных, сведений о работающих сотрудниках.
- Криптографические. Специальные системы шифрования и кодировки, которые используются для защиты информации при телефонных переговорах, рабочих встречах, в рамках совещаний. Принцип работы криптографии состоит в применении математических моделей кодировки сообщений, что обеспечивает эффективную защиту информации от несанкционированного изменения и использования злоумышленниками.

Благодаря техническим средствам, обеспечивающим защиту информации, предприятие может не только детально проработать и протестировать новые разработки и технологии, но и успеть запатентовать их. ИТЗ снижает риск промышленного шпионажа и плагиата нового изделия, поэтому защита компьютерной информации – первостепенная задача для любой компании.

Основные виды инженерно-технической защиты информации

ИТЗ также можно классифицировать следующим образом:

- по способу реализации;
- по классам средств злоумышленника;
- по масштабу охвата;
- по конкретным объектам, на которые направлено воздействие;
- по характеру мероприятий;
- по классу систем для инженерной защиты.

Комплексные меры по защите информации

Говоря о защите конфиденциальных данных, нельзя обойти стороной использование комплексного подхода. Практика показывает, что делая ставку только на одну из систем нельзя добиться 100% защищенности информации. Неудивительно, что сегодня системы технических средств, направленных на контроль за информацией, постоянно совершенствуются.

В дорыночный период существования нашей страны производство представляло собой систему замкнутых структур, которая обеспечивала своеобразную защиту информации от утечки, хотя они все равно происходили. Тотальный контроль и отсутствие взаимодействия с западными учеными замедляли научно-технический прогресс. Многие инновационные на тот период времени проекты так и не были реализованы из-за отсутствия взаимодействия ведомств между собой.

Комплексные меры по защите информации

Конечно, в условиях капиталистического рынка нельзя реализовывать такую защиту, поскольку компания должна иметь возможность рекламировать свою продукцию, приоткрывая тем самым завесу тайны. Однако активное использование средств инженерной технической защиты информации снижает риск причинения ущерба компании.

Подводя итоги об инженерно-технической защите информации, стоит заметить, что не все предприятия оснащены эффективной системой противодействия хищению данных. Своевременное внедрение современных комплексов и инженерно-технических систем защиты информации позволяет свести утечки к минимуму, обеспечив эффективное функционирование организации.

Методы и средства инженерной защиты объектов информатизации

Инженерная защита предназначена для механического воспрепятствования проникновению злоумышленника к объектам защиты. Она включает инженерные конструкции, создающие механические преграды на пути злоумышленника, и комплексы управления доступом людей и автотранспорта на охраняемую территорию.

Инженерные конструкции, несмотря на бурное развитие электронных средств охраны, вносят основную долю в эффективность системы ИЗТООИ, так как злоумышленник вынужден большую часть времени тратить на преодоление механических барьеров на пути к объекту зашиты. А чем больше время перемещения его на охраняемой территории, тем выше вероятность его обнаружения и нейтрализации. Поэтому в период ухудшения криминогенной обстановки частные лица и организации направляют основные свои усилия на укрепление инженерных конструкций (дверей, окон, стен, заборов и т.д.).

Методы и средства инженерной защиты объектов информатизации

Мало мест осталось на земле, где хозяева, уходя, не закрывают двери своих жилищ. Забор с воротами для территории и дверь с замком для помещения применяют в любой организации и в любом доме. В общем случае к инженерным конструкциям и сооружениям для защиты информации относятся:

- Естественные и искусственные преграды (барьеры) на возможном пути движения злоумышленника к источникам информации или другим ценностям;
- Двери, ворота и окна зданий и помещений;
- Контрольно-пропускные пункты (КПП) для контролируемого пропуска на охраняемую территорию людей и автотранспорта;
- Шкафы и рабочие столы с закрываемыми на ключ ящиками;
- Хранилища, металлические шкафы и сейфы.

Методы и средства инженерной защиты объектов информатизации

К естественным преградам относятся неровности поверхности земли (рвы, овраги, скалы и др.), труднопроходимые лес и кустарник на границах территории организации.

Искусственные преграды существенно отличаются по конструкции. Они выполняются в виде бетонных или кирпичных заборов, решеток или сеточных конструкций, металлических оград, конструкций для ограничения скорости проезда транспортных средств и др. Бетонные и кирпичные заборы, как правило, имеют высоту в пределах 1,8—2,5 м, сеточные — до 2,2 м. Для создания злоумышленнику дополнительных препятствий сверху кирпичных и бетонных заборов укрепляют защитную (колючую) проволоку, острые стержни или битое стекло.

Для защиты верхней части капитальных заборов применяется также армированная колючая лента.

Методы и средства инженерной защиты объектов информатизации

Для предотвращения проникновения злоумышленника через забор и крышу, ограничения доступа на отдельных подходах, создания полосы отчуждения вдоль забора, здания и сооружения эффективны малозаметные проволочные сети. Вариант сети представляет собой проволочное плетение в виде пространственной четырехъярусной сети размером 10х5х1,4 м, выполненной из кольцевых гирлянд диаметром 0,5—0,6 м и соединенных между собой по длине и высоте отдельными скрутками из мягкой проволоки. Диаметр проволоки составляет 0,5—0,9 мм.

На объектах с высоким уровнем защиты устанавливают две линии искусственных барьеров на расстоянии 1 — 1,5 м друг от друга или применяют сочетание искусственных и естественных барьеров (рвов, оврагов, водоемов и др.), если таковые имеются.

Кроме создания механических препятствий, барьеры оказывают психологическое отпугивающее воздействие на малоквалифицированных злоумышленников.

Методы и средства инженерной защиты объектов информатизации

Двери и ворота — традиционные конструкции для пропуска людей или транспорта на территорию организации или в помещение. В зависимости от требований к уровню защиты устанавливаются деревянные или металлические двери.
Надежность дверей определяется не только их толщиной, механической прочностью материала двери и средств крепления дверной рамы к стене, но и надежностью замков. За свою историю люди придумали разнообразные замки. Современные замки можно классифицировать следующим образом:

- механические, открываемые (закрываемые) механическим ключом;
- механические кодовые;
- электромеханические;
- электронные кодовые.

Дверные замки делятся на врезные, накладные и навесные. Взлом-стойкость замков зависит от конструкции, типа металла и секретности запорного механизма, оцениваемой количеством комбинаций положений штифтов или кодовых комбинаций. Чем больше количество комбинаций, тем выше его стойкость от различного рода отмычек. Число комбинаций ключа замка должно быть не менее 10 106 и 3* 106 для замковых устройств классов B. C и D соответственно.

Методы и средства инженерной защиты объектов информатизации

Сейфовые замки бывают сувальдного типа с количеством сувальд не менее 8 и сложным профилем бородок ключа, кодовыми механическими, временными и электронными. Самые распространенные кодовые замки — дисковые кодовые с секретностью КГ6—107 комбинаций.

Наибольшую стойкость имеют электронные замки с ключами в виде электронных карточек типа Touch Memory. Электронный идентификатор этого вида представляет микросхему, размешенную в герметичном корпусе из нержавеющей стали. Корпус имеет цилиндрическую форму диаметром 16 мм и высотой 3—5 мм. Такой корпус устойчив к воздействию агрессивных сред, влаге, грязи и механическим нагрузкам. Кроме зашиты, корпус микросхемы выполняет роль контактной группы: один контакт — крышечка и боковая поверхность, другой — изолированное металлическое донышко. Каждая микросхема имеет неизменяемый 64-разрядный номер, определить который перебором практически невозможно — около Ю20 комбинаций. Механическая устойчивость замков обеспечивается за счет удлиненных горизонтальных и вертикальных ригелей.

Методы и средства инженерной защиты объектов информатизации

Электрозащелки представляют собой ответную часть замка и используются совместно с обычным механическим замком. При подаче управляющего напряжения разблокируется фиксатор электрозащелки, и дверь может быть открыта при выдвинутом положении ригеля механического замка. При этом используемый механический замок не должен открываться снаружи поворотом ручки. При наличии ручки с внутренней стороны двери она может быть открыта изнутри поворотом ручки без подачи управляющего напряжения на защелку.

Окна, особенно на 1—2-м этажах зданий, являются слабым местом в системе инженерной зашиты. Их укрепляют двумя основными способами:

1. применением специальных, устойчивых к механическим ударам стекол;
2. установлением в оконных проемах металлических решеток.

Вместо обычного строительного стекла, которое легко разбивается на осколки, применяют полузакаленное, закаленное и многослойное стекло. Полузакаленное стекло в 2 раза более прочное, чем обычное строительное, но разбивается оно аналогично строительному. Закаленное стекло приблизительно в 4 раза прочнее обычного строительного. При разбивании оно полностью раскалывается на мельчайшие кусочки.

Методы и средства инженерной защиты объектов информатизации

Многослойное стекло состоит обычно из двух стекол, которые склеиваются прочной синтетической пленкой. Оно может быть изготовлено из обычного строительного, полу- и закаленного стекла. Многослойное стекло защищает от насильственного вторжения, даже если удары по стеклу неоднократно наносятся молотком, ломом или кирпичом. Кроме того, это стекло нельзя вырезать только с одной стороны, что лишает злоумышленника возможности бесшумно проникнуть в помещение, используя стеклорезы.

Технологическим прорывом стало применение так называемых ламинированных пленок с высоким сопротивлением на разрыв и нового синтетического клея, обеспечивающего надежное сцепление на молекулярном уровне пленки со стеклом. На основе этих пленок созданы противоударные и противовзломные стекла высокой устойчивости. Кроме того, между пленками могут размещаться тонкие металлические провода, подключаемые в качестве электроконтактных датчиков средств охраны.

Для повышения прочности стекол применяются также различные защитные оконные пленки, которые приклеивают к внутренней или внешней поверхности окон в зависимости от решаемой задачи.

Методы и средства инженерной защиты объектов информатизации

Решетки устанавливаются на тех окнах, через которые возможен легкий доступ в помещение здания. К ним относятся, прежде всего, окна на первом или последнем этажах здания, вблизи наружных лестниц или близко расположенных больших деревьев. Металлические решетки бывают бескаркасные, прутья которых заделываются непосредственно в стену, и каркасные — прутья привариваются к металлической раме, а рама затем крепится к стене. Диаметр прутьев не менее 10 мм (обычно 15 мм), расстояние между ними составляет порядка 120 мм, глубина заделки их в стену — не менее 200 мм.

Методы и средства инженерной защиты объектов информатизации

Для пропуска людей и автомобилей на территорию организации создают автоматизированные или автоматические контрольно-пропускные пункты (КПП): проходные для людей и проездные для транспорта.

В типовом варианте КПП включает:

- Зал со средствами управления доступом для прохода людей;
- Бюро пропусков;
- Камеру хранения вещей персонала и посетителей, не разрешенных для проноса в организацию;
- Помещения для начальника охраны, дежурного контролера, размещения охранной сигнализации и связи и другие;
- Средства управления доступом транспорта.

Конструкция, состав и количество КПП определяются размерами территории организации и количеством персонала. КПП должны обеспечивать необходимую пропускную способность людей и транспорта. Запасные входы и проезды для пропуска людей и транспорта в аварийной ситуации в нормальных условиях закрываются, пломбируются или опечатываются.

Методы и средства инженерной защиты объектов информатизации

КПП содержат механизмы системы контроля доступа (турникеты, раздвижные или поворачивающиеся двери, шлюзы, ворота, шлагбаумы для авто- и железнодорожного транспорта и др.), а также системы идентификации людей.

Системы контроля доступа являются сложными и многоплановыми электронными системами безопасности, поэтому точно и однозначно сформулировать их назначение непросто. По сути, обычная дверь с механическим замком или механический турникет с вахтером тоже являются своего рода системами контроля доступа. Прежде всего, электронные системы контроля доступа обеспечивают возможность доступа определенных лиц в определенные помещения и ограничивают доступ лиц, не имеющих права доступа в соответствующие зоны.

Методы и средства инженерной защиты объектов информатизации

Простейшими электронными системами доступа являются кодонаборные панели или автономные считыватели карточек. Более сложные системы, включающие, как правило, один или несколько компьютеров, могут контролировать доступ в зависимости от текущего времени, дня недели и праздничных дней. Такая система ведет протокол всех происшедших событий проходов определенного пользователя через определенную дверь в определенное время, попыток несанкционированного доступа и т.д.

Программное обеспечение позволяет получить различные виды отчетов о событиях, происшедших в системе за определенный отрезок времени. Кроме того, различные системы могут иметь широкий набор дополнительных функций, например, защита от несанкционированного проникновения в помещение путем передачи карты другому лицу, графическое представление на экране компьютера плана объекта с отображением тревожных ситуаций и т.д.

В качестве исполнительных устройств системы контроля доступа могут использоваться электрозамки различных типов, турникеты, автоматические двери и т.п. Объектом доступа может быть не только человек, но и автомобиль с закрепленным на нем специальным устройством. Исполнительными механизмами доступа в этом случае являются шлагбаумы и автоматические приводы ворот.

Методы и средства инженерной защиты объектов информатизации

Кроме своей прямой функции разграничения доступа, компьютеризированные системы могут использоваться для автоматического учета рабочего времени, контроля прохождения заданного маршрута охранником, управления различными устройствами (сиренами, освещением и т.п.). Многие системы позволяют подключать датчики охранной и пожарной сигнализации и вырабатывать сигнал тревоги или управлять системой видеонаблюдения. Например, при попытке входа в помещение нелегального пользователя (предъявлении системе нелегальной карты) включится видеомагнитофон и зафиксирует действия злоумышленника.

При всем многообразии возможных структур построения систем контроля доступа все они построены на базе идентификации чего-либо. Идентификация может строиться на самых разных физических принципах.

Методы и средства инженерной защиты объектов информатизации

Кодовые клавиатуры — наиболее простые устройства доступа. Идентифицируется код, набираемый пользователем. Индивидуальный для каждого пользователя код позволит системе понять, кто именно его набирает. Знание кода достаточно для «обмана» системы, но код нельзя потерять, его можно только сообщить (добровольно или под угрозой). Многие модели имеют дополнительные функции повышения секретности: выработка сигнала тревоги при попытке подбора кода, специальный код, подающий сигнал тревоги, и т.д. Совмещенные считыватели, например «карта + код», обеспечивают защиту в случае утери карты легальным пользователем, для доступа надо не только предъявить карту, но и набрать код.

Магнитные карты — наиболее широко и давно известный тип карт. Многие системы позволяют использовать стандартные кредитные карточки с магнитной полосой. Для считывания необходимо расположить карточку определенным образом и провести ее через считыватель, это не всегда удобно и требует определенного времени. Карты и считыватели имеют достаточно большой, но вполне конечный ресурс. Загрязнение карты, размещение вблизи сильных источников магнитного поля может привести к выходу ее из строя.

Методы и средства инженерной защиты объектов информатизации

Карты Виганда (Wigand) представляют собой пластиковую карточку, в которую при изготовлении запрессованы хаотично расположенные отрезки проволочек из специального магнитного сплава. Проведение карты мимо магнитной головки дает определенный код, индивидуальный для каждой карты. Такие карты значительно более износоустойчивы, чем магнитные, надежно защищены от подделки и копирования, но дороже магнитных и требуют определенного позиционирования относительно считывателя.

Методы и средства инженерной защиты объектов информатизации

Бесконтактные (Proximity) карты обеспечивают считывание кода просто при поднесении карточки к считывателю на определенное расстояние, при этом позиционирование карточки относительно считывателя не имеет значения. Расстояние для большинства считывателей составляет 5—15 см, а для некоторых моделей считывателей достигает 1—2 м. Отсутствие необходимости позиционировать карту обеспечивает простоту и высокую скорость прохода пользователя, что особенно важно при частом использовании карты и на проходных в условиях интенсивного потока пользователей. Карточка абсолютно не изнашивается, не имеет источника питания, не боится влаги, загрязнения, обладает достаточной механической прочностью, неограниченным сроком службы. Проксимити-карточки обычно программируются при изготовлении, но есть модели с возможностью перезаписи кода. По формату стандартная карта соответствует обычной магнитной карточке, но чуть толще. Существуют «тонкие» проксимити, полностью соответствующие по размеру стандартной магнитной карте. На проксимити-карты могут наноситься надписи и фотографии.

Методы и средства инженерной защиты объектов информатизации

По той же технологии изготавливаются идентификаторы в виде брелков, браслетов или специальных устройств, закрепляемых на автомобилях. Идентификаторы проксимити могут иметь встроенный источник питания. При этом их срок службы составляет не менее 5 лет, и удается достигнуть большого радиуса действия при меньших размерах считывателя.

Методы и средства инженерной защиты объектов информатизации

Штрих-код — карточки содержат штрих код (Barcode), нанесенный на бумажную или пластиковую основу. Для считывания карточки ее необходимо определенным образом провести через прорезь считывателя, где установлены светочувствительные элементы. Основной недостаток — легкость копирования и подделки. Несколько труднее подделать карточки со штрих-кодом, видимым только в инфракрасном диапазоне, — нужны видеокамера (она чувствительна в ИК-диапазоне) или прибор ночного видения.

Радиоканальныеустройства — могут использоваться для передачи кода считывателю. Идентификатором может служить миниатюрный радиобрелок или небольшой передатчик, установленный на автомобиле. Достаточной степенью защищенности обладают только специальные системы с «блуждающим» кодом, остальные системы достаточно легко «взламываются». Преимущество — большой радиус действия. Обычно используются для управления воротами, шлагбаумами и т.п.

ИК-брелки — миниатюрные передатчики кода в инфракрасном диапазоне. Они лучше, чем радиоканальные устройства, защищены от перехвата, за счет большей направленности и меньшего радиуса. Находят очень ограниченное применение.

Методы и средства инженерной защиты объектов информатизации

Смарт-карты — карты формата обычной кредитки, имеют встроенный процессор и контактные площадки для питания и обмена со считывателем. Могут иметь очень высокую степень защищенности, но в системах контроля доступа находят крайне ограниченное применение.

Электронные ключи — различные устройства, содержащие код и передающие его считывателю через контакты. Наибольшее распространение получили брелки и карты touch memory производства фирмы Dallas Semiconductor. Микросхема с кодом расположена в миниатюрном корпусе из нержавеющей стали, конструктивно напоминающем батарейку «таблетка». Для передачи кода необходимо коснуться такой «таблеткой» контактов считывателя. Выпускаются в оправках в виде брелка или крепятся к карточке стандартного формата. Имеют крайне высокую износостойкость, механическую прочность, устойчивы к агрессивным средам.

Биометрические системы распознавания основаны на анализе индивидуальных биометрических признаков человека: отпечатков пальцев, тембра голоса, рисунка сетчатки глаза, формы кисти руки. В настоящее время идут исследования возможности применения биометрических систем распознавания по расположению зубов (стоматологической матрице) ротовой полости человека.

Методы и средства инженерной защиты объектов информатизации

Турникеты являются традиционными и одними из важнейших исполнительных механизмов систем контроля доступа. Они применяются для оборудования входов в помещения или ограничения входа в отдельные части помещений, а ряд моделей может использоваться для ограничения входа на территорию. Для управления электромеханическими турникетами, кроме пультов ручного управления, могут использоваться любые устройства контроля доступа: считыватели карточек различного типа, электронные ключи, радиобрелки, клавиатуры, приемники жетонов и т.д. Это значительно расширяет область применения турникетов и позволяет включать их в состав сетевых компьютеризированных систем контроля доступа. Турникет является в некоторой степени уникальным исполнительным устройством системы контроля доступа, так как обеспечивает проход людей «по одному», в отличие от двери, оборудованной электрозамком.

Методы и средства инженерной защиты объектов информатизации

Ведь предъявив считывателю карточку, пользователь может не только пройти сам, но и впустить человека, не имеющего права доступа в соответствующее помещение. Это прямое нарушение, но представьте себе следующую ситуацию: пользователь подходит к двери, оборудованной считывателем карточек и электрозамком, предъявляет считывателю карточку и получает доступ, он открывает дверь и должен ее закрыть «перед носом» идущего следом за ним. Это может быть не всегда удобно, но проявление вежливости обернется нарушением самого принципа санкционированного доступа. Эта проблема снимается, если речь идет о внутренних помещениях объекта, где все присутствующие являются пользователями системы санкционированного доступа и понимают причину подобной «невежливости», но на входах и выходах из контролируемых зон только турникет в состоянии решить проблему пропуска «по одному».

Методы и средства инженерной защиты объектов информатизации

Трипод — турникет с вращающимися преграждающими планками. Трипод является наиболее популярным типом турникета. Это обусловлено его невысокой стоимостью, компактностью, возможностью гармонично вписать в любой интерьер. Трипод обладает относительно невысокой степенью секретности в сравнении с более сложными моделями — через преграждающую планку можно перелезть или проползти под ней. Однако такой турникет, как правило, устанавливается в местах постоянного присутствия сотрудника охраны. Кроме того, повысить безопасность можно установкой инфракрасных датчиков, срабатывающих при попытках перелезть через турникет или проникнуть под преграждающей планкой. В этом случае срабатывание датчика вызовет сигнал тревоги, который может быть подан на сирену, в помещение охраны или включит видеозапись действий злоумышленника.

Полупрофильный турникет — конструктивно напоминает хорошо знакомую «вертушку». Обеспечивает большую степень защищенности, чем трипод, но требует большего пространства для установки.

Методы и средства инженерной защиты объектов информатизации

Калитка — турникет, выполненный в виде калитки. Существуют модели с моторизованным приводом — калитка открывается автоматически при подаче соответствующего управляющего сигнала, и модели, в которых управляющий сигнал разблокирует калитку и позволяет открыть ее вручную. Сама калитка, как правило, выполнена из металлических труб или стекла.

Скоростные турникеты — обеспечивают более высокую пропускную способность. Они могут иметь конструкцию с дверцами небольшой высоты или высокими створками, обеспечивающими повышенную степень секретности. Скоростные модели могут, как правило, работать в режиме «постоянно открыт», т.е. створки в исходном положении открыты и закрываются только при попытке несанкционированного прохода (аналогично установленным в Московском метрополитене).

Полнопрофильные турникеты — турникеты, обеспечивающие максимальную степень секретности. Они имеют конструкцию в полный рост человека, могут быть выполнены в виде вращающихся брусьев, вращающихся стеклянных створок и т.п. Ряд моделей предназначены для установки на улице и обеспечивают контроль доступа на охраняемые территории.

Методы и средства инженерной защиты объектов информатизации

Доводчики двери служат для принудительного закрытия двери и обеспечивают надежную работу электрозамков. Подавляющее большинство типов доводчиков используют гидравлическое демпфирование для достижения плавности хода двери. Регулирующие клапаны позволяют выбрать требуемую скорость закрывания двери. Различные модели предназначены для дверей разного размера (массы). Модели также отличаются конструктивным исполнением, дизайном, рядом дополнительных функций: фиксация двери в положении «открыто», ускорение в завершающей фазе закрывания — «прихлоп» и т.д.

Контрольно-проездные пункты для пропуска авто- и железнодорожного транспорта оборудуются:

- Раздвижными или распашными воротами и шлагбаумами с механическим, электромеханическим и гидравлическим приводами, а также устройствами для аварийной остановки ворот и открывания их вручную;
- Контрольными площадками с помостами для просмотра автомобилей;
- Светофорами, предупредительными знаками и световыми табло типа «берегись автомобиля» и др.;
- Телефонной и тревожной связью и освещением для осмотра автотранспорта.

Методы и средства инженерной защиты объектов информатизации

Весьма надежными и широко применяемыми средствами зашиты документов, продукции и других ценностей являются металлические шкафы, сейфы и хранилища.

Металлические шкафы предназначены для хранения документов с невысоким грифом конфиденциальности, ценных вещей, небольшой суммы денег. Надежность шкафов определяется только прочностью металла и секретностью замка.

Для хранения особо ценных документов, вещей, больших сумм денег применяются сейфы и хранилища. К сейфам относятся двустенные металлические шкафы с тяжелыми наполнителями пространства между стенками, в качестве которых используются армированные бетонные составы, композиты, многослойные заполнители из различных материалов.

Хранилище представляет собой сооружение с площадью основания внутреннего пространства более 2 м, защищенное от взлома и устойчивое к воздействию высокой температуры при пожаре.

Стойкость хранилищ и сейфов оценивается в условных единицах сопротивления, которые определяются как произведение времени взлома на коэффициент сложности применяемого для этого инструмента с учетом сложности его доставки и использования.