Физическая безопасность ответственных объектов

Сузанн Найлз (Suzanne Niles)

Информационная статья № 82

Legendary Reliability®

Revision 1

Краткий обзор

Физическая безопасность — или контроль доступа персонала — чрезвычайно важна с точки зрения достижения целевых значений уровня готовности вычислительного центра. По мере распространения новых технологий, включая средства биометрической идентификации и дистанционного управления данными систем безопасности, традиционные карточки / ключи и охранники вытесняются системами, способными обеспечивать идентификацию с подтверждением и контролировать деятельность людей в помещениях ВЦ и вблизи него. Прежде чем покупать оборудование, менеджеру IT необходимо тщательно взвесить потребности и определить наиболее подходящий и экономичный набор мер для своей системы. Настоящая статья включает обзор принципов идентификации персонала и описание основных элементов и процедур, применяемых в системах обеспечения безопасности.

Введение

Человеческий фактор: риск, требующий контроля

Первые ассоциации при упоминании о безопасности вычислительного центра — саботаж, шпионаж или хищение данных. Сомневаться в необходимости защиты от вторжений и намеренного вреда, который может стать их следствием, не приходится, однако для большинства ВЦ значительно более существенны риски повседневной деятельности сотрудников.

Обойтись вообще без персонала невозможно, однако все исследования неизменно говорят о том,что человеческий фактор — отклонения от утвержденных процедур, ошибки в маркировке, оброненные предметы и пролитые жидкости, опечатки при наборе команд с клавиатуры и прочие мелкие и крупные непредвиденные неприятности — является прямой причиной 60% всех простоев ВЦ. Ошибки — неизбежные спутники человека, и минимизация и контроль доступа персонала в производственные помещения являются критически важным элементом управления рисками, даже когда вероятность злонамеренных действий минимальна.

Технологии идентификации меняются так же быстро, как и защищаемые сооружения, средства информационных и коммуникационных технологий. Чрезмерное увлечение все новой аппаратурой и технологиями может заставить забыть о том, что извечная проблема, для решения которой они предназначаются: держать лишних и злонамеренных людей подальше от мест, где им быть не положено, — не является ни технической, ни сложной. И даже если на первом шаге — при составлении карты охраняемых зон и разработке правил доступа в них — могут получаться сложные многоуровневые схемы, они не противоречат интуитивным представлениям. Администраторы IT, в общем случае, и так знают, кому нужно бывать и где. Проблему представляет второй шаг: определение наилучшего варианта применения менее совершенных технологий для решения поставленных задач.

Инженерная инфраструктура центра обработки данных

Средства обеспечения физической безопасности напрямую влияют на уровень готовности системы и продолжительность ее бесперебойной работы (учитывая простои из-за различных происшествий или саботажа, обусловленных присутствием излишнего персонала или злоумышленников), что требует рассматривать их как часть *Инженерной инфраструктуры центра обработки данных* (ИИЦОД).

В состав ИИЦОД входят также стойки для монтажа оборудования, средства питания, охлаждения, организации кабелей и пожаротушения.

Кто вы такой, и что вам здесь нужно?

Пускай новые технологии обеспечения безопасности выглядят иногда экзотическими и загадочными — смарт-карты, идентификация по отпечаткам пальцев, ладоням, радужной оболочке глаза, геометрии лица — решаемая ими задача остается неизменной с тех пор, как у людей появилось что защищать. Она проста и знакома каждому: как получить достоверный ответ на вопрос «Кто вы такой, и что вам здесь нужно?»

Первая часть вопроса — «кто вы такой?» — представляет наибольшую сложность при создании автоматизированных систем обеспечения безопасности. Все современные технологии предполагают идентификацию личности различными способами, отличающимися по степени надежности и цене. Например, карточные замки недороги, но не обеспечивают идентификации личности (невозможно быть уверенным в том, кто именно воспользовался карточкой); сканер радужной оболочки глаза стоит очень дорого, но обеспечивает высокую надежность идентификации. Поиск приемлемого компромисса между надежностью и ценой — коренной вопрос проектирования системы обеспечения безопасности.

Ответ на вторую часть вопроса — «что вам здесь нужно?», или, другими словами, какова ваша роль — может следовать из ответа на первую автоматически (например, «Это Эллис Уилсон, наш специалист по кабельному хозяйству; она работает с кабелями — впустить ее»). Возможны и другие варианты. Например, идентификационная информация и сведения о выполняемой роли могут быть записаны совместно на одной и той же карточке с магнитной полосой; может использоваться база данных, содержащая необходимые сведения о персонале; или для контроля доступа в различные зоны могут применяться различные средства, с учетом их специфики. Иногда первая часть вопроса, вынесенного в заголовок раздела, вообще не имеет значения. Достаточно знать, что человек собирается делать — например, если это ремонтник или уборщик.

Соединение знаний и опыта различных специалистов для поиска решений

Менеджеры IT всегда знают «кто и что» на их объекте, но могут не вполне разбираться в деталях современных технологий или способов их применения — но это и не обязательно. Вполне достаточно владения информацией об ограничениях бюджета и рисках, связанных с различными нарушениями безопасности на конкретном объекте.

Другое дело — консультант по средствам обеспечения безопасности, который не может вникать в особенности каждого объекта, но зато досконально разбирается в преимуществах и недостатках существующих технологий, а также в затратности их применения. Кроме того, он или она обладает опытом проектирования систем безопасности и может помочь добиться ясности, уточнить и упростить требования, связанные с решением вопроса «кто и что», вовремя задавая правильные вопросы.

Соединив свои знания и опыт, эти специалисты могут разработать систему, сбалансированную с учетом требований ограничения доступа, приемлемости рисков, возможностей существующих технологий и бюджетных ограничений.

Постановка задачи

Зоны безопасности: что требует защиты?

Первый шаг в проектировании системы обеспечения безопасности — составление плана объекта и обозначение на нем областей, требующих различных **уровней безопасности**, а также путей проникновения в эти области, требующих различных правил доступа.

Такие зоны могут находиться одна внутри другой:

периметр земельного участка,
периметр здания,
зона размещения оборудования IT,
компьютерные залы,
стойки с аппаратурой, —

или граничить друг с другом:

зона для посетителей,
офисная зона,
служебные помещения.

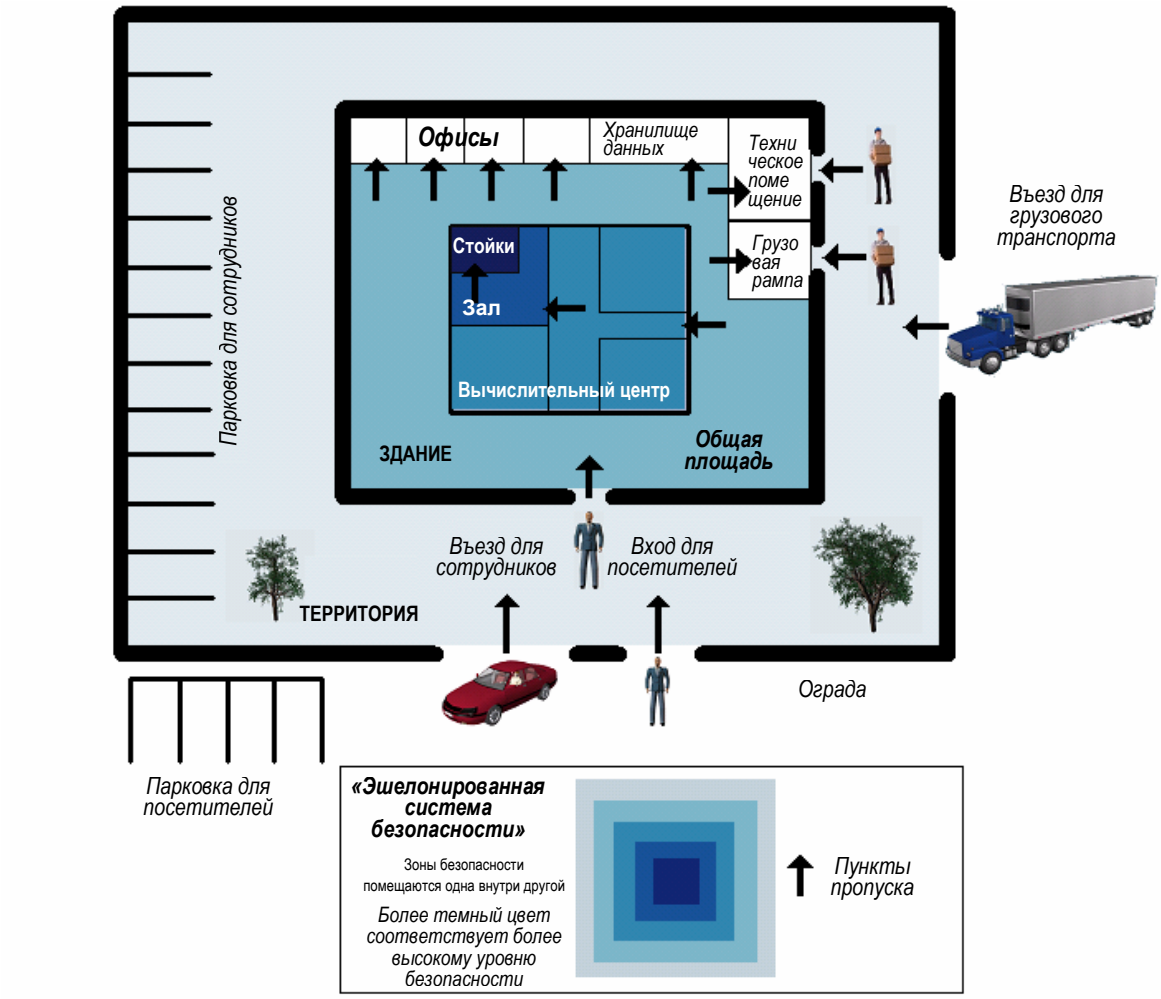
«Физическая безопасность» может также означать…

Термин *физическая безопасность* может применяться также к средствам защиты при катастрофических событиях (пожарах, наводнениях, землетрясениях, бомбардировках) или при авариях коммунальных сетей (отключение электроснабжения, отказ систем кондиционирования воздуха).

В настоящей статье он используется только для обозначения защиты от вторжения на объект посторонних.

В первом случае возможно **эшелонированное построение системы безопасности**, когда на каждой следующей границе применяется иной набор технологий либо последовательно все более жесткие меры контроля доступа. Таким образом зона, находящаяся внутри других, оказывается защищена не только мерами на своей собственной границе, но и на границах окружающих ее зон. Кроме того, нарушение безопасности на внешней границе может быть скомпенсировано дополнительными мерами в следующем эшелоне.

Рисунок 1 *– План объекта с «эшелонированной истемой безопасности»*



Безопасность на уровне стойки. Самый глубокий «эшелон безопасности» — глубже уровня серверного зала — уровень *стойки*. Дверцы стоек (пока) редко оснащаются замками, но при наличии таких замков они служат последним рубежом обороны от неавторизованного доступа к ответственной аппаратуре. Маловероятно, чтобы каждому, имеющему допуск в зал, заставленный стойками с аппаратурой, был необходим доступ к ним всем; использование замков гарантирует, что специалисты по обслуживанию серверов будут иметь доступ только к серверам, по телекоммуникационной аппаратуре — только к ней, и т.д. «Администрируемые» замки стоек дистанционно конфигурируются таким образом, чтобы открывать их могли только определенные люди в определенное время. Это снижает риск различных происшествий, саботажа или неавторизованной установки дополнительного оборудования, что ведет к потенциально опасному росту потребления электроэнергии и температуры в стойке.

Безопасность на уровне инфраструктуры. На плане объекта со схемой системы безопасности необходимо отмечать не только места установки оборудования IT, но и области размещения компонентов инженерной инфраструктуры, повреждение или иное воздействие на которые может вести к простоям. Например, аппаратура кондиционирования воздуха может оказаться случайно или намеренно отключена, аккумуляторы запуска генератора — украдены, а консоль системного администрирования может включить систему пожаротушения по ошибочному сигналу.

Критерий контроля доступа: кого допускать куда?

Предоставление конкретному специалисту права доступа в ту или иную зону может зависеть от различных факторов. Помимо таких очевидных, как личность и цель, — первые два в списке ниже — возможны дополнительные, требующие особого отношения («особый случай»).

Личность. Определенные лица, известные на объекте, нуждаются в доступе к определенным зонам по своей должности. Например, директору службы безопасности необходимо бывать на большей части территории объекта, но не в местах хранения клиентских данных. Глава службы эксплуатации вычислительной техники может быть допущен в серверные залы, но не в технические помещения, где располагаются системы питания и кондиционирования воздуха. Главному исполнительному директору компании может потребоваться допуск в офисы директора службы безопасности ВЦ и специалистов IT, а также на общие площади, но не в серверные залы или технические помещения.

Не смешивайте различные вопросы

Не следует допускать, чтобы особенности конкретных технологий идентификации находили отражение в составляемом на первом этапе списке требований безопасности. В первую очередь необходимо определить зоны безопасности и критерии допуска в них, *затем* выполнить анализ затрат / эффективности / рисков, рассмотреть возможные компромиссы и выбрать наилучший состав и вариант реализации технологий.

Цель. Ремонтник, независимо от того, зовут ли его Джо Смит или это женщина по имени Мэри Джонс, может нуждаться в доступе только в технические помещения и на общие площади. Уборщики, списочный состав которых нередко меняется каждый день, должны допускаться на общие площади, но никуда больше. Специалисту по сетевым коммутаторам может быть предоставлен доступ к стойкам с коммутационным оборудованием, но не с серверами или устройствами хранения. В центре хостинга веб-серверов специалистам по обслуживанию клиентских систем может предоставляться доступ только в «комнаты клиентского доступа», куда выведены консоли управления используемых ими серверов.

Особый случай. Доступ в зоны, требующие особенно жесткой защиты, может предоставляться только конкретным людям и для конкретных целей — т.е., если они нуждаются в доступе по «особому случаю», и только на время, пока такая потребность сохраняется.

Применение технологий

Технологии идентификации: надежность и цена

Технологии идентификации личности можно поделить на три основных категории, в порядке повышения надежности — и цены оборудования:

- **Что у вас есть.**
- **Что вы знаете.**
- **Кто вы.**

Что у вас есть *Низший уровень надежности (возможна передача или хищение)*

Идентификация производится по некоторому предмету, носимому на себе или с собой — ключу, карточке или идентификатору, который может быть встроен, например, в брелок. Он может быть «простым», как старомодный металлический ключ, или «умным», как карточка со встроенным процессором, который обменивается информацией со считывающим устройством (**смарт-карта**). Это может быть карточка с магнитной полосой, на которой записана информация о ее владельце (такая как хорошо всем знакомая карточка для получения денег из банкомата), а также карточка или идентификатор со встроенным передатчиком / приемо-передатчиком для обмена информацией со считывающим устройством на небольшом расстоянии (примером могут служить распространенные устройства Mobil Speedpass®).

Средства идентификации категории *что у вас есть* наименее надежны, поскольку нет никакой гарантии, что идентифицируемый предмет не сменил владельца — ведь его легко передать, украсть или потерять и найти.

Что вы знаете *Более высокий уровень надежности (украсть нельзя, но возможно передать или прочесть запись знания, если она существует)*

Знать можно пароль, код или некоторую процедуру — например, последовательность открывания кодового замка, процедуру использования считывающего устройства или открывания сеанса работы с компьютером с клавиатуры. Пароль / код ставит перед специалистом по безопасности дополнительную дилемму: легко запоминающуюся комбинацию, скорее всего, нетрудно будет подобрать, а плохо запоминающиеся пользователи, обычно, записывают, и эту запись может прочесть посторонний.

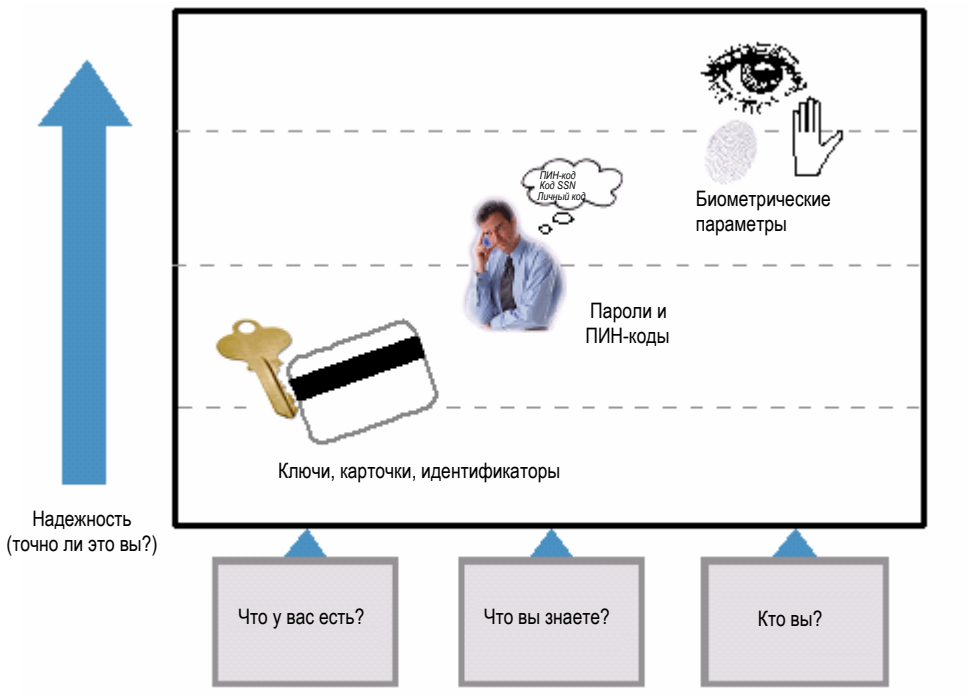
Средства идентификации данной категории более надежны, но пароль или код все же может быть передан другому человеку, а записанный где-либо для памяти — обнаружен и прочитан.

Кто вы *Высший уровень надежности (используются уникальные биометрические характеристики человека)*

Оцениваются уникальные физические характеристики человека — этот способом люди сами почти безошибочно узнают друг друга. Его копирование (или попытка копирования) техническими средствами называется **биометрией**. Уже созданы технологии оценки ряда биометрических характеристик человека, хорошо поддающихся числовому представлению и анализу:

Палец (рисунок папиллярных линий).
Радужная оболочка глаза (цветовой рисунок).
Глазное дно (рисунок кровеносных сосудов).
Голос.
Рука (форма пальцев и толщина ладони).
Лицо (геометрия глаз, носа и рта в их взаимном расположении).
Почерк (динамика движения пера).

Рисунок 2 *– Что у вас есть, что вы знаете, кто вы?*



Биометрические устройства, в целом, обеспечивают очень высокую надежность положительной идентификации — то есть, если устройство вас опознало, это почти наверняка *действительно* вы. Главный источник ненадежности биометрии — не ошибочная положительная идентификация, или опознание постороннего как зарегистрированного пользователя, а вероятность ошибочного неопознания зарегистрированного пользователя («ошибочная отрицательная идентификация»).

Сочетание различных методов для повышения надежности

Типичная схема обеспечения безопасности использует последовательно все более надежные — и дорогие — методы идентификации от внешней (наименее защищенной) к внутренним (более защищенным) зонам. Например, для входа в здание может быть достаточно карточки и ПИН-кода; а на входе в компьютерный зал потребуется еще набрать правильную комбинацию кодового замка и пройти биометрическую идентификацию. Сочетание различных методов идентификации повышает уровень надежности; применение в более глубоких эшелонах методов, отличных от используемых на внешних, значительно укрепляет безопасность внутренних зон, которые оказываются защищены как своими собственными средствами, так и мерами защиты окружающих их зон.

Почему все так сложно?

Причина видимой сложности систем обеспечения заключается в том, что пока не создано технологии, которая позволяла бы быстро, легко, недорого и безошибочно идентифицировать человека. Существует лишь набор методов различной эффективности, удобства и стоимости, что делает необходимым сложный анализ стоимости/эффективности/рисков и совместное применение различных технологий либо построение эшелонированной защиты периметров.

Управление системой безопасности

Некоторые средства контроля доступа — в частности, считывающие устройства и биометрические сканеры — могут использоваться также для сбора данных, например, о том, кто и когда проходил идентификацию. При подключении к сети эта информация может передаваться в систему управления для целей мониторинга и ведения регистрационных журналов (прихода и ухода), управления устройствами (конфигурирования для пропуска определенных людей в определенные периоды времени) и выдачи тревожных уведомлений (о повторных безуспешных попытках авторизации и об отказах устройств).

Устройства контроля доступа

Карточки и идентификаторы: «что у вас есть»

В настоящее время для контроля доступа используются различные типы карточек и идентификаторов различной степени сложности устройства, отличающиеся наличием и степенью развития дополнительных возможностей, таких как:

- возможность программирования;
- защита от подделки;
- тип контакта со считывающим устройством: пропуск через щель, вставка в специальное гнездо, плоскостной контакт, без непосредственного контакта («бесконтактные»);
- удобство: форм-фактор и возможные способы ношения с собой / на себе;

- объем хранимых данных;
- вычислительные возможности;
- стоимость карточки или брелка;
- стоимость считывающего устройства.

Независимо от того, насколько надежны и защищены эти устройства, обеспечиваемый ими уровень безопасности ограничен отсутствием гарантий использования именно тем человеком, за которым они числятся. Поэтому такие устройства, обычно, применяются в сочетании с одним или несколькими дополнительными методами идентификации: парольными или даже биометрическими.

Карточка с магнитной полосой — наиболее распространенный тип карточек, использующий для хранения идентификационных данных полоску магнитного материала. При ее пропуске через щель считывающего устройства выполняется запрос к базе данных. Система недорога и удобна; ее недостатком является сравнительная простота подделки и считывания хранимой информации вне целевой системы.

Феррит-бариевая карточка (также называемая «карточкой с магнитными метками») сходна с карточкой с магнитной полосой, но обеспечивает более надежную защиту при несколько более высокой цене. Она содержит тонкий слой магнитного материала с расположенными определенным образом круглыми участками. Вместо сканирования или пропуска через щель ее просто прикладывают к считывающему устройству.

Карточка Weigand представляет собой разновидность карточки с магнитной полосой. Внедренный в нее пучок намагниченных проволочек образует уникальную магнитную сигнатуру. При пропуске такой карточки через щель считывающего устройства в индуктивном датчике наводится ток, который преобразуется в последовательность битов. Преимущество этого более сложного устройства карточки состоит в невозможности подделки; а недостаток — в невозможности перепрограммирования. Непосредственный контакт с датчиком считывающего устройства не обязателен, что позволяет создавать герметизированные конструкции, подходящие для установки вне помещений. В отличие от считывающих устройств для бесконтактных карт и карточек с магнитной полосой, устройства системы Weigand не подвержены электромагнитным и радиочастотным помехам. Неприхотливость оборудования в сочетании со сложностью подделки карты делает систему Weigand чрезвычайно защищенной (в пределах общих ограничений метода «что у вас есть»), но она и более затратна.

Карточка со штрихкодом несет на себе штрихкод, считываемый при пропуске через щель сканера. Система отличается исключительно низкой ценой, но практически не защищена от подделки — получить работоспособную копию карточки можно с помощью обычного копира. Эта технология защиты хороша при минимальных требованиях безопасности, в особенности если на объекте устанавливается большое число считывающих устройств или при большом трафике через пункт пропуска. Она применяется не столько для обеспечения безопасности, сколько для *мониторинга* доступа. (Говоря простым языком, система защиты на базе штрих-кода — это замок «от честных людей».)

Инфракрасная просветная карточка обеспечивает более высокий уровень защиты благодаря помещению штрихкода между слоями ПВХ. Считывание производится на просвет в инфракрасном диапазоне.

Бесконтактная карта — более удобна, по сравнению с карточками, требующими пропуска через щель считывающего устройства. Как следует из названия, непосредственный контакт со сканером не обязателен — достаточно поднести к нему карту на некоторое небольшое расстояние. Используется технология радиочастотной идентификации (RFID). Радиоизлучение необходимой мощности обеспечивает считывающее устройство. Наиболее популярные варианты работают на расстоянии около 10 см.; существует также разновидность — называемая **картой дистанционной идентификации** — рассчитанная на расстояние около метра.

Смарт-карта — одно из последних достижений в области карточных систем контроля доступа — быстро выходит в лидеры по популярности при развертывании новых систем. Встроенный в такую карточку полупроводниковый кристалл служит для хранения данных и / или производства вычислений. Обмен данными может производиться при контакте со считывающим устройством (*контактная* смарт-карта) или дистанционно, с использованием той же технологии, что и в бесконтактных картах и картах дистанционной идентификации (*бесконтактные* смарт-карты и смарт-карты *дистанционной идентификации*). Использование карточки стандартного формата не обязательно — полупроводниковый кристалл имеет диаметр около сантиметра-полутора и может встраиваться, например, в удостоверение личности с фотографией, брелок, металлическую «таблетку» или ювелирное украшение (как идентификаторы iButton®). Собирательно такие устройства называют *смарт-идентификаторами.*

Смарт-карты обеспечивают большую гибкость в контроле доступа. Например, полупроводниковый кристалл можно встроить в карточку другого типа для интеграции с существующей системой безопасности или ее поэтапной модернизации. Большой объем хранения позволяет записать сведения об отпечатке пальца или рисунке радужной оболочки глаза законного владельца карты — в этом случае совместное использование считывающего устройства и средств биометрической идентификации позволяет перевести систему безопасности из категории «что у вас есть» в категорию «кто вы». Смарт-карты дистанционной идентификации обеспечивают максимальное удобство для пользователя: вся процедура занимает около половины секунды, и карточку даже не нужно извлекать из бумажника.

Кодовые и комбинационные замки: «что вы знаете»

Кодовые и **комбинационные замки** широко применяются для контроля доступа. Эти устройства отличаются надежностью и удобны для пользователей, но обеспечиваемый ими уровень защиты ограничен возможностью передачи или подбора пароля. Для ввода кода используется клавиатура, практически не отличающаяся от хорошо всем знакомой телефонной. Если код уникален для каждого пользователя, он называется персональным кодом доступа (ПКД) или персональным идентификационным номером (ПИН). *Кодовый замок*, обычно, позволяет вводить множество различных кодов, выделяя каждому пользователю индивидуальный; а *комбинационным замком*, как правило, называют устройство, использующее один код на всех.

Уровень безопасности при использовании кодовых и комбинационных замков можно повысить периодической сменой кодов, что требует некоторой схемы оповещения пользователей и распространения новых кодов. Если этот прием не используется, необходимо время от времени менять сами клавиатуры, чтобы исключить появление выдающих код признаков износа клавиш. Как и в случае с карточками, качество защиты можно повысить с помощью средств биометрической идентификации.

Биометрия: «кто вы»

Биометрические технологии быстро развиваются, становясь все лучше и дешевле. Высоконадежные, доступные по цене средства биометрической верификации — прежде всего по отпечатку пальца — выходят на основные позиции в арсенале обеспечения безопасности. Многие производители поставляют в настоящее время широкий спектр биометрических устройств, дополнение которыми существующих систем категорий «что у вас есть» и «что вы знаете» позволяет выйти на уровень передовых стандартов контроля доступа.

Как правило, средства биометрической идентификации применяются не для *идентификации* путем поиска соответствия в БД пользователей, а для *верификации* личности, идентифицированной с применением технологий категорий «что у вас есть» или «что вы знаете» — например, идентификация производится по карточке / ПИН-коду, а затем выполняется верификация по отпечатку пальца. Очевидно, со временем повышение производительности и надежности биометрических технологий сделает возможным создание средств *идентификации* личности на их основе без привлечения карточных, парольных или иных дополнительных средств.

Почему не ограничиться *только* биометрией?

Вопрос: Для чего использовать на пункте пропуска, оснащенном средствами биометрической идентификации, еще и карточки и ПИН-коды? Почему не ограничиться только биометрией, если она так надежна?

Ответ: Потому что (1) если выполнять сравнение со всеми записями в БД, а не только с одной, при большом числе зарегистрированных пользователей время обработки запроса может оказаться неприемлемо велико; (2) риск ошибочной отрицательной идентификации при биометрическом контроле моно снизить, если сравнение выполнять только с одной записью в базе данных.

Хотя подделать биометрические характеристики практически невозможно, из-за несовершенства технологии остается некоторый риск ошибочной положительной идентификации.

Различают два типа ошибок при биометрической идентификации:

Ошибочная отрицательная идентификация. — Неопознание зарегистрированного пользователя. Можно, конечно, рассуждать о том, что эта ошибка является следствием усиленной заботы о безопасности, но недопуск зарегистрированного пользователя из-за ошибки сканера — очень большое неудобство.

Ошибочная положительная идентификация. — За зарегистрированного пользователя может быть ошибочно принят другой зарегистрированный пользователь либо вообще посторонний человек.

Ошибки обоих типов взаимосвязаны, и вероятность одних можно снижать за счет повышения вероятности других. Достаточно изменить значение порога распознавания («процента сходства, являющегося основанием для положительной идентификации»).

Принимать решение об использовании биометрических технологий необходимо с учетом стоимости оборудования, вероятности ошибки каждого типа и *приемлемости для пользователей*. Последняя характеристика относится к тому, насколько утомительна, неудобна или даже опасна используемая процедура с точки зрения идентифицируемого. Например, сканеры радужной оболочки в общем случае мало приемлемы для пользователей из-за необходимости приблизить глаз на 3-5 см к объективу, через который выполняется сканирование лучом светодиода.

Рисунок 3 *– Сканер формы руки*

Другие элементы системы безопасности

Главный вопрос проектирования систем безопасности — выбор оборудования для идентификации и классификации входящих («контроля доступа»). Собственно, *при условии* 100-процентной надежности идентификации, отсутствии сомнений в надежности людей, которым разрешен доступ, прочности стен, полов и потолков и надежности дверей, окон, замков этот вопрос был бы также и единственным. Для противодействия опасностям, сопряженным с неизбежными несовершенствами или саботажем, системы безопасности, обычно, оснащаются дополнительными средствами защиты, мониторинга и ликвидации нарушений.

Конструкция здания

При строительстве нового объекта или реконструкции существующего необходимо с самого начала закладывать в проект все меры защиты, включая применение архитектурных и строительных решений, препятствующих вторжению или делающих его более затруднительным. Основные соображения по безопасности, которые необходимо учитывать при проектировании здания и его инженерного оснащения, относятся к возможным маршрутам проникновения и отхода, доступу к важнейшим элементам инфраструктуры, таким как системы вентиляции и кондиционирования, кабельная проводка, а также к местам, где может укрыться нарушитель. Более подробный список некоторых таких соображений приведен в приложении.

Несанкционированный провод и проход: тамбуры

Распространенная досадная лазейка в надежных в остальном системах контроля доступа — возможность провода или прохода второго человека вслед за идентифицированным (при соучастии этого первого — он может, например, придержать дверь — или без его ведома). Традиционное решение этой проблемы — **тамбур** с пространством между входной и выходной дверьми, достаточным только для одного человека. Средства контроля доступа могут устанавливаться на обеих дверях тамбура или только на выходной — в последнем случае неудачная попытка идентификации может влечь за собой блокировку обеих дверей и выдачу сигнала о поимке нарушителя. Кроме того, подсчет шагов с помощью специального датчика позволяет проверить, не вошел ли в тамбур лишний человек.

Новая технология решения этой проблемы — видеокамера, соединенная с компьютером, который обнаруживает на изображении входящих и выдает сигнал тревоги при попытке прохода более одного человека на разрешающий сигнал.

Фотосъемка и видеонаблюдение

Фотокамеры могут использоваться для фиксации номеров автомобилей в пунктах пропуска и, в сочетании с датчиками шагов, для фотографирования людей на важных участках.

Камеры видеонаблюдения — установленные скрытно или открыто — могут использоваться для ведения наблюдения в помещении или на прилегающей к зданию территории, как средство сдерживания и для последующего анализа происшествий. Могут использоваться камеры различных типов: фиксированные, поворотные или дистанционно управляемые. Вот некоторые соображения по выбору мест установки камер:

- Нужна ли возможность идентификации людей, попадающих в поле зрения камеры?
- Достаточно ли просто определить, есть кто-то в помещении или нет?
- Является ли целью наблюдения обнаружение пропажи ценностей?
- Предназначена ли камера служить просто средством сдерживания?

Если ведется запись сигнала с камер видеонаблюдения, необходимо решить следующие вопросы:

- Индексирование и каталогизация записей для удобства выборки.
- Хранение записей на объекте или вне его.
- Составление списка лиц, имеющих доступ к записям.
- Процедура доступа к записям.
- Продолжительность хранения записей.

Новые технологии позволяют автоматизировать работу, традиционно выполняемую сотрудниками охраны, — наблюдение за происходящим на экранах мониторов — с использованием программного обеспечения, обнаруживающего изменения (движение) на телевизионной картинке.

Охранники

При всех технологических достижениях в области физической безопасности специалисты сходятся во мнении, что штат квалифицированных охранников стоит на первом месте в списке резервных и вспомогательных средств контроля доступа. Охранники могут вести наблюдение с использованием всех человеческих органов чувств, а кроме того — реагировать на подозрительные, необычные или опасные события, используя свою мобильность и интеллект.

Неправительственная организация Международный фонд работников охраны (International Foundation for Protection Officers, IFPO), основанная с целью стандартизации профессионального обучения и сертификации, публикует справочное руководство *Security Supervisor Training Manual* для охранников и их нанимателей.

Датчики и тревожная сигнализация

Всем знакомы системы сигнализации и их датчики, традиционно применяемые для охраны жилых помещений и зданий: датчики движения, тепла, контактные пары (используемые для определения открывания дверей) и т.п. В системах сигнализации ВЦ помимо перечисленных могут и применяться дополнительные типы датчиков — лазерные барьеры, датчики шагов, прикосновений, вибрации. Кроме того, в определенных зонах вычислительного центра может быть предпочтительно не использовать звуковые сигналы тревоги, чтобы легче было застать нарушителей «с поличным».

Если датчики подключаются к сети, оказывается возможным дистанционный мониторинг и управление ими в рамках системы управления и администрирования, получающей от средств контроля доступа также информацию о перемещениях персонала (см. пункт **Управление системой безопасности** выше).

Посетители

При проектировании системы безопасности всегда необходимо предусматривать работу с посетителями. Обычно для прохода в зоны с низким уровнем безопасности им выдаются временные значки или карточки, а посещение зон с высоким уровнем безопасности допускается только в сопровождении. При использовании тамбуров (предназначенных для предотвращения прохода двух человек по одной авторизации) оказывается необходим механизм временного отключения этой меры безопасности либо генерация отдельных реквизитов для посетителей.

Человеческий фактор

Технические средства не могут самостоятельно выполнять всю работу, в особенности такую человеческую по своей сути, как узнавание людей и оценка их намерений. Хотя человеческий фактор является важнейшей частью проблемы безопасности, он же является и частью ее решения: человеческие достоинства и недостатки делают персонал одновременно и слабым звеном и лучшей резервной системой обеспечения безопасности.

Персонал: слабое звено

В дополнение к ошибкам и несчастным случаям присутствует риск, связанный с естественным человеческим дружелюбием и доверчивостью. Знакомый с охраной и другими сотрудниками человек может оказаться недовольным бывшим работником или агентом конкурирующей компании; соблазн отступить от установленных правил или пренебречь обязательными процедурами ради знакомого лица нередко приводит к катастрофическим последствиям; важная категория нарушений в области безопасности приходится как раз на такие «внутренние угрозы». Даже совершенно посторонним людям удается удивительно успешно преодолевать барьеры системы безопасности с помощью некоторых несложных хитростей и приемов. Эти технологии хорошо известны и документированы и даже уже получили собственное название: **социальная инженерия**. Каждый сотрудник в зоне, где возможно причинение вреда, должен быть хорошо обучен не только протоколам работы и режима безопасности, но и противодействию изобретательным приемам социальной инженерии.

Персонал: лучшая резервная система

Защита от нарушений режима безопасности часто сводится к распознаванию и интерпретации неожиданных событий — дело, в котором технике с людьми не сравниться. Прибавьте к этому непоколебимую сопротивляемость манипулированию и обходным маневрам, и вы увидите, что присутствие человека может быть бесценным дополнением к работе машин.

Помимо использования бдительности основного персонала несравненная ценность глаз, ушей, способности к суждениям и мобильности позволяет включать человека в систему обеспечения безопасности специальным отдельным элементом — в форме старомодного охранника. Присутствие охранников в пунктах пропуска и патрулирование территории и здания, хотя и дорого обходится, может спасти ситуацию при отказе технических средств обеспечения безопасности или их преодолении теми или иными способами. Оперативная реакция охранника в ситуациях, когда «что-то идет не так», может оказаться последним рубежом обороны против потенциально катастрофических нарушений режима безопасности.

Вклад человека в дело защиты от случайного или намеренного причинения вреда тот же самый: постоянная бдительность и строгое следование протоколам. После удаления всех, чье присутствие не является необходимым для работы объекта, оставшийся персонал — хорошо обученный, следующий продуманным схемам и процедурам — оказывается последним рубежом эффективной системы обеспечения физической безопасности.

Выбор решения: баланс рисков и затрат

Правильно спроектированная система безопасности — это оптимальный компромисс между рисками и потенциальным ущербом от присутствия лишних людей с одной стороны и затратами сил и средств на меры безопасности, направленные на их недопущение в защищаемые зоны.

Потенциальная цена нарушения режима безопасности

Каждый вычислительный центр уникален по масштабам и другим характеристикам возможного ущерба, однако в большинстве случаев присутствуют следующие категории:

Материальный ущерб — повреждение помещений и оборудования вследствие несчастных случаев, саботажа или прямых хищений.

Потери рабочего времени персонала IT— отвлечение специалистов от основных обязанностей на ремонт или замену оборудования, восстановление данных и исправности систем.

Потери рабочего времени специалистов по основной деятельности — приостановка ведения бизнеса из-за простоев ВЦ.

Потеря информации — утрата, повреждение или хищение данных.

Ущерб для репутации и утрата расположения клиентов — серьезные или повторные нарушения режима безопасности могут приводить к потере бизнеса, снижению курса акций, юридическим осложнениям.

Соображения по проектированию систем обеспечения безопасности

Проектирование систем обеспечения безопасности может представлять собой сложное уравнение со множеством переменных. Хотя рассмотрение конкретных стратегий в этой области не входит в задачи настоящей статьи, обычно необходимо бывает решить следующие вопросы:

Стоимость оборудования — как правило, применение высоконадежных средств идентификации ограничивается бюджетом. Обычный подход к решению этой проблемы заключается в применении на каждом участке своих технологий, в зависимости от предъявляемых требований по уровню безопасности.

Сочетание технологий — надежность идентификации на любом уровне может быть повышена комбинированием технологий различной стоимости. При эшелонированной защите каждый следующий эшелон оказывается защищен также средствами обеспечения безопасности всех предыдущих.

Приемлемость для пользователей — (фактор «беспокойства»). Простота в использовании и надежность идентификации играют важную роль в предотвращении недовольства системой и возникновения соблазна искать обходные пути.

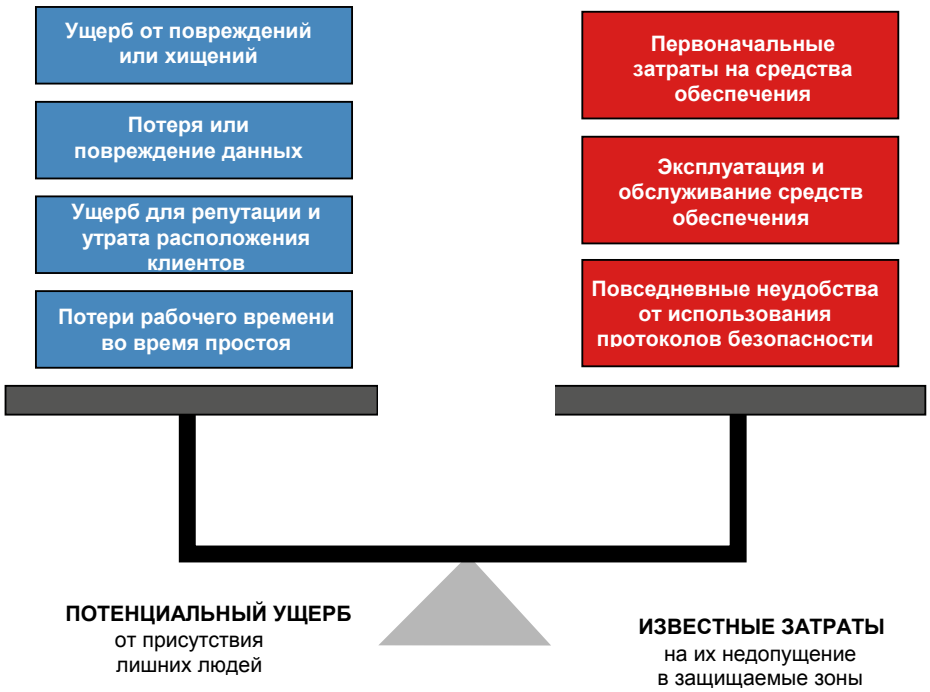
Не все можно купить

Даже если деньги — не проблема, окружение объекта сплошным щитом безопасности в большинстве случаев создает неприемлемые трудности и неудобства. Необходимо реально оценить потребность в защите каждой из зон с учетом того, что именно требует защиты и кому необходим доступ.

Масштабируемость — возможность поэтапного развертывания системы, по мере необходимости, поступления средств или укрепления уверенности в применяемых технологиях.

Обратная совместимость — совместимость нового проекта с сохраняемыми элементами существующей системы безопасности. Сохранение всей или части существующей системы, обычно, позволяет значительно удешевить проект.

Рисунок 4 *– Баланс потенциального ущерба и стоимости защиты*



Заключение

С увеличением числа вычислительных центров и центров хостинга веб-сайтов потребность в обеспечении физической безопасности этих объектов оказывается ничуть не меньше, чем в мерах кибербезопасности сетей. Нарушители, выдающие себя за других людей или скрывающие свои действительные цели, способны причинить огромный ущерб: от физического вывода из строя ответственного оборудования до осуществления атаки на программном уровне с использованием незащищенной консоли. Даже обычные ошибки вполне благонамеренного персонала представляют значительную повседневную угрозу работе центра, а ограничение присутствия людей самым необходимым позволяет ее минимизировать.

Соответствующие технологии уже существуют, и стоимость их применения постоянно снижается. Они позволяют реализовывать широкий диапазон решений, опирающихся на принципы идентификации **что у вас есть**, **что вы знаете** и **кто вы**. Соединение оценки рисков с анализом требований к контролю доступа и ассортимента имеющихся технологий позволяет спроектировать эффективную систему обеспечения безопасности, основанную на реалистическом балансе уровня защиты и цены.

Об авторе

Сузанн Найлз — автор информационных статей в научно-инженерном центре APC Engineering Design Center в Биллерике, шт. Массачусетс.Она изучала математику в колледже Веллесли, получила степень бакалавра в области вычислительной техники в Массачусетском технологическом институте, защитив работу о распознавании рукописного текста.Ведет преподавательскую деятельность более 25 лет, работает с различными аудиториями, используя самые разные обучающие материалы: от руководств по программному обеспечению до фотографий и детских песен. До поступления на работу в APC в 2004 г. Найлз занимала должность редактора в издательстве The Village Group, где работала над новой книгой Веса Кассмола (Wes Kussmaul) *«Счастье покоя» (Quiet Enjoyment)*, посвященной вопросам безопасности и идентификации личности в эпоху Интернета.

Приложение

Вопросы безопасности в проектировании зданий

При строительстве нового объекта или реконструкции существующего необходимо с самого начала закладывать в проект все меры защиты, включая применение архитектурных и строительных решений, препятствующих вторжению или делающих его более затруднительным. Основные соображения по безопасности, которые необходимо учитывать при проектировании здания и его инженерного оснащения, относятся к возможным маршрутам проникновения и отхода, доступу к важнейшим элементам инфраструктуры, таким как системы вентиляции и кондиционирования, кабельная проводка, а также к местам, где может укрыться нарушитель.

Вопросам безопасности в выборе площадки для строительства посвящена информационная статья APC №81 «Site Selection for Mission Critical Facilities» («Выбор площадок для ответственных сооружений»).

- Вход в вычислительный центр следует размещать, по возможности, на удалении от маршрутов движения людей и грузов, не ведущих к самому ВЦ или от него.
- Используйте стальные двери и коробки со сплошными, а не полыми полотнами. Петли должны быть защищены от воздействия снаружи.
- Для внутренних стен в здании ВЦ следует использовать более прочные материалы, нежели применяются обычно. Кроме того, в них можно закладывать датчики для обнаружения попыток проникновения.
- Помещения вычислительного центра не должны выходить на внешние стены.
- С постов охраны и точек установки камер видеонаблюдения должен открываться максимально полный и незатрудненный обзор.
- Используйте визуальные барьеры, чтобы скрыть входы и другие части ВЦ от обзора извне. Эта мера призвана помешать исследованию внутреннего устройства здания и мер безопасности без проникновения через защищаемые периметры.
- Возьмите на учет все вентиляционные оголовки и каналы, грузовые люки, шахты лифтов и другие проемы и отверстия, которые могут использоваться для проникновения. На все такие отверстия, имеющие более 30 см в поперечнике, необходимо установить решетки.
- Избегайте создания мест, где нарушитель мог бы укрыться сам или разместить какие-либо предметы. Например, таким местом может служить пространство под фальшполом. Обеспечьте защиту возможных укрытий и сделайте их малозаметными для людей, проходящих по помещениям.

- Установите замки и датчики открывания на все люки и другие точки доступа с крыши, чтобы ни одна попытка проникновения не осталась незаметной. Число таких точек доступа необходимо свести к минимуму.

- Возьмите на учет все подводы внешних коммуникаций: канализации, кабельных сетей, системы вентиляции и кондиционирования воздуха и т.п., — и позаботьтесь об их защите. Расположенные открыто или без надлежащей защиты, эти компоненты инфраструктуры предоставляют возможности для саботажа функционирования объекта без преодоления его системы безопасности.

- Исключите доступ к внутренней проводке, канализационным и вентиляционным каналам изнутри здания. Как бы ни тщательно был защищен вычислительный центр, если из коридора можно добраться до силовой или информационной проводки, его безопасность под угрозой.

- При реконструкции существующего ВЦ либо размещении нового на существующем объекте необходимо тщательно продумать его планировку. Избегайте создания уязвимых зон или рисков, связанных с человеческим фактором. Например, не следует размещать ВЦ под кухнями, производственными помещениями с тяжелым оборудованием, парковками и зонами, по которым проходят большие потоки людей или транспорта, а также рядом с ними. Угрозу может представлять что угодно, от пожара на кухне до взрывчатки в автомобиле или автомобильной аварии.

- В остеклении центрального поста наблюдения необходимо использовать пуленепробиваемое стекло.

- Если ВЦ располагается в отдельном здании, избегайте признаков, выдающих его назначение. Не размещайте на стенах, на крыше или ограде надписей, содержащих названия компаний или логотипы, по которым можно было бы понять, что в здании находится вычислительный центр.

- Используйте бетонные блоки и другие препятствия для предотвращения приближения к зданию нежелательных транспортных средств.

Словарь терминов

В тексте статей **жирным шрифтом** выделены термины, включенные в настоящий словарь.

Бесконтактная карта,

Бесконтактная карточка

Тип карточек, применяемых для **контроля доступа**. Оснащается приемопередатчиком **RFID** для обмена данными со считывающим устройством на расстоянии до 1 м.

Бесконтактная смарт-карта

Смарт-карта, использующая технологию **RFID** для обмена информацией со считывающим устройством без непосредственного контакта. В зависимости от используемого стандарта RFID максимальная рабочая дистанция может составлять около 10 см или около 1 м (**дистанционные** бесконтактные смарт-карты).

Биометрический замок

Замок, управляемый биометрическим сканером.

Биометрия

Идентификация личности с применением технологий численной оценки физических или поведенческих характеристик — например, отпечатка пальца.

Вероятность ошибочной положительной идентификации

Для биометрического устройства, процент сканирований, завершающихся **ошибочной положительной идентификацией.**

Геометрия лица

Внешние признаки, допускающие числовую оценку с применением биометрических технологий — например, взаимное расположение глаз, носа и рта.

Готовность

Расчетный процент времени, в течение которого система находится в рабочем состоянии. Для ответственных объектов целевым является уровень готовности в «пять девяток», или 99,999% — что соответствует менее чем 5 минутам простоя в год.

Дистанционная карта

Тип карточек, применяемых для **контроля доступа**, со встроенным приемо-передатчиком **RFID**, используемым для обмена данными со считывающим устройством на расстоянии до 1 м.

Эшелонированная система безопасности

Набор вложенных защищаемых периметров, из которых внешний (например, периметр здания) защищен в наименьшей, а самый внутренний (например, периметр стойки с аппаратурой) — в наибольшей степени.

Эшелонированная система защиты

Система, в которой периметры защищаемых зон вложены один в другой, а для их защиты используются различные либо последовательно все более жесткие меры контроля доступа. Зона, находящаяся внутри других, оказывается защищена не только мерами на своей собственной границе, но и на границах окружающих ее зон.

ИИЦОД

Инженерная инфраструктура центра обработки данных. Различные элементы инженерной инфраструктуры вычислительного центра (в отличие от инфраструктуры IT, включающей такие устройства, как маршрутизаторы и контроллеры хранения), оказывающие непосредственное влияние на уровень **готовности** путем обеспечения бесперебойной работы. ИИЦОД охватывает средства питания, охлаждения, пожаротушения и **физической безопасности**.

Идентификатор

Небольшой предмет со встроенном микрочипом, используемым для хранения персональных идентификационных данных. В зависимости от используемых технологий, может быть необходимо приложить идентификатор к считывающему устройству либо просто поднести к нему на некоторое расстояние (**RFID**-идентификаторы).

Инженерная инфраструктура центра обработки данных — см. ИИЦОД

Инфракрасная просветная карточка

Тип карточек, применяемых для **контроля доступа**. Содержит штрихкод, помещенный между слоями пластика. Считывание производится на просвет в инфракрасном диапазоне.

Карточка с магнитной полосой

Тип карточек, применяемых для **контроля доступа**. Информация хранится на полоске магнитного материала и считывается при пропуске через щель считывающего устройства.

Карточка со штрихкодом

Тип карточки, используемой для **контроля доступа**. Идентификационная информация хранится в виде штрихкода. Считывание происходит при пропуске карточки через щель считывающего устройства.

Карточка Weigand

Тип карточек, применяемых для **контроля доступа**. Для хранения информации используется пучок специальным образом обработанных и намагниченных проволочек. Считывание данных осуществляется при пропуске карточки через щель считывающего устройства.

Кодовый замок

Замок, открываемый нажатием на кнопки в определенной последовательности. Отличается от **комбинационного замка** тем, что обычно имеет лишь 4-5 кнопок, каждая из которых нажимается при открывании только один раз. Комбинационный замок с металлическими кнопками является механическим предшественником современного электронного кодового замка с клавиатурой телефонного типа.

Комбинационный замок

Замок, открываемый вводом определенного кода с клавиатуры.

Контактная смарт-карта

Смарт-карта, требующая непосредственного контакта со считывающим устройством. Ср. С **бесконтактной смарт-картой**.

Контроль доступа

Контроль доступа людей в здания, помещения и к стойкам с оборудованием, а также использования ими оборудования и консолей с применением автоматизированных систем, считывающих информацию с карточки или иного идентификатора (**что у вас есть**), принимающих коды или пароли (**что вы знаете**) или оценивающих биометрические характеристики человека (**кто вы**).

Кто вы

В **контроле доступа** — категория методов идентификации, основанных на уникальных биологических или поведенческих особенностях человека. Эти методы наиболее надежны, поскольку оцениваемые характеристики очень трудно подделать; однако их надежность не достигает 100%, в основном из-за ошибок измерения и анализа. Другое название данной группы методов идентификации — **биометрия**.

Несанкционированный провод

Нарушение режима безопасности, при котором авторизованный пользователь проводит через **пункт пропуска** вместе с собой неавторизованного — например, придерживая для него дверь. (Сходное нарушение — **несанкционированный проход**, при котором неавторизованный пользователь незаметно проскальзывает через **пункт пропуска** вслед за авторизованным.)

Несанкционированный проход

Нарушение режима безопасности, при котором неавторизованный пользователь незаметно проскальзывает через **пункт пропуска** вслед за авторизованным. (Сходное нарушение —**несанкционированный провод**, при котором авторизованный пользователь проводит неавторизованного через **пункт пропуска**, например, придерживая для него дверь.)

Образ

В **биометрии** — числовое представление оцениваемой характеристики, требующее меньше пространства для хранения, чем необработанные данные сканирования, но сохраняющее индивидуальность. Такие образы хранятся в базах данных авторизованных пользователей и в памяти **смарт-карт** и используются для сравнения с данными сканирования, полученными в **пункте пропуска**.

Особый случай

Основание для предоставления доступа в зоны с высоким уровнем защиты только определенным людям, только для определенных целей (например, для получения конкретных данных) и только на период времени, пока в этом сохраняется потребность.

Отпечаток голоса

В **биометрии** — числовое представление голоса пользователя, используемое для сравнения с его голосом в **пункте пропуска**.

Ошибочная отрицательная идентификация

При биометрической идентификации — ошибка, состоящая в неопознании зарегистрированного пользователя. Другой тип ошибки биометрической идентификации — **ошибочная положительная идентификация.**

Ошибочная положительная идентификация

При биометрической идентификации — ошибка, состоящая в идентификации как зарегистрированного пользователя другого человека. Другой тип ошибки биометрической идентификации — **ошибочная отрицательная идентификация**.

ПКД

Персональный код доступа. Альтернативное название для ПИН (персонального идентификационного номера) — кода, или пароля, используемого для идентификации пользователя в **пункте пропуска**.

Порог

В **биометрии** — регулируемый параметр, позволяющий менять соотношение вероятностей взаимозависимых ошибок двух типов (**ошибочная положительная идентификация** и **ошибочная отрицательная идентификация**). Поскольку он представляет собой «процент сходства, являющегося основанием для положительной идентификации», снижение вероятности ошибки одного типа автоматически влечет за собой повышение вероятности ошибки другого типа.

Пункт пропуска

Участок периметра защищенной зоны, оборудованный дверью или воротами и теми или иными средствами **контроля доступа**, применяемыми к любому, кто попытается пройти или проехать.

Сканирование глазного дна

Технология биометрической идентификации, использующая числовое выражение рисунка сетки сосудов на сетчатке глаза.

Сканирование радужной оболочки

Технология биометрической идентификации, использующая числовое выражение цветового рисунка радужной оболочки глаза.

Сканирование формы руки

Технология биометрической идентификации, использующая числовое выражение трехмерной геометрии руки — формы пальцев и толщины ладони.

Смарт-идентификатор

Небольшой предмет произвольной формы, содержащий полупроводниковый кристалл того же типа, что применяется в **смарт-картах**. Обычно такие идентификаторы встраиваются в брелки или в ювелирные украшения.

Смарт-карта

Тип карточек, применяемых для **контроля доступа**. Информация хранится в памяти полупроводникового кристалла, который, кроме того, способен производить определенные вычисления и обмениваться данными со считывающим устройством. Смарт-карта прикладывается к считывающему устройству таким образом, чтобы их электрические контакты соединились. См. также пункт **бесконтактная смарт-карта**.

Социальная инженерия

Применение некоторых несложных хитростей и приемов для избежания предусмотренных режимом безопасности процедур. Например, выманивание паролей, одалживание ключей, просьбы открыть или придержать дверь.

Тамбур

Тамбур с пространством между защищенными входной и выходной дверьми, достаточным только для одного человека. Применяется для предотвращения прохода нарушителя вместе с авторизованным пользователем.

Управление

Автоматический обмен данными и командами с удаленными устройствами в процессе мониторинга, управления и подачи тревожных сигналов. Этот новый термин *управление*, сходный с традиционными терминами «автоматизация инфраструктуры здания» и «автоматизация жилого помещения», применяется к обмену по сети данными и командами со всеми элементами вычислительного центра, включая само оборудование IT (серверы, устройства хранения, телекоммуникационная аппаратура и сетевые устройства) и физическую инфраструктуру (средства питания, охлаждения, противопожарной защиты и безопасности).

Управляемый

Допускающий дистанционный мониторинг и управление. Управляемые устройства **контроля доступа** взаимодействуют с удаленными системами управления в процессе *мониторинга* (кто пришел и когда), *управления* (конфигурирования устройств для пропуска определенных людей в определенные промежутки времени) и *подачи тревожных сигналов* (уведомление о повторных неудачных попытках прохода и об отказах устройств).

Феррит-бариевая карточка

Тип карточки, используемой для **контроля доступа**. Идентификационная информация хранится в виде рисунка намагниченных областей. Считывание происходит при прикладывании к рабочей поверхности считывающего устройства. Также называется «карточкой с магнитными метками».

Физическая безопасность

Защита физических объектов от несчастных случаев и саботажа, являющихся следствием присутствия посторонних или злоумышленников. Система физической безопасности всегда включает устройства **контроля доступа**, обеспечивающие автоматический контроль на **пунктах пропуска**, и системы сигнализации на основе датчиков. В состав дополнительных средств защиты могут входить системы видеонаблюдения и посты охраны. (Иногда термин *физическая безопасность* трактуется более широко и охватывает защиту ото всех видов физических угроз, включая атмосферные стихийные бедствия, землетрясения, военные действия. В настоящей статье он применяется для обозначения защиты только от неприятностей, вызванных неавторизованным присутствием на объекте *людей*.)

Что вы знаете

В **контроле доступа** — категория методов идентификации, основанных на том, что пользователь располагает некоторой информацией, например паролем или цифровым кодом. Такие средства идентификации более надежны, чем относящиеся к категории **что у вас есть,** но пароль или код все же может быть передан другому человеку, а записанный где-либо для памяти — обнаружен и прочитан.

Что у вас есть

В **контроле доступа** — категория методов идентификации, основанных на наличии у пользователя некоторого предмета, такого как карточка или **идентификатор**. Методы этой категории наименее надежны, поскольку нет никакой гарантии, что идентифицируемый предмет не сменил владельца.

iButton®

Микрочип, подобный применяемым в **смарт-картах**, но заключенный в металлическую «таблетку» диаметром около сантиметра-полутора, которую можно встроить в брелок или в ювелирное украшение. Устройства iButtons отличаются исключительной прочностью и стойкостью к неблагоприятным воздействиям но (по состоянию на май 2004) не используют технологию **RFID** и не поддерживают бесконтактного взаимодействия.

IFPO

International Foundation for Protection Officers. Международный фонд работников охраны — некоммерческая организация, основанная с целью стандартизации профессионального обучения и сертификации, публикует справочное руководство *Security Supervisor Training Manual* для охранников и их нанимателей.

RFID

Radio frequency identification, радиочастотная идентификация. Технология, предусматривающая взаимодействие карточки и считывающего без физического контакта. Технология RFID используется в **бесконтактных картах**, **дистанционных картах** и **бесконтактных смарт-картах**. Микросхема RFID получает необходимую энергию от луча считывающего устройства, что позволяет обходиться без собственного источника питания.