1. Лекция: Определение информационной безопасности

Вводится общее понятие информационной безопасности, рассматривается краткая история ее развития. Анализируются современные стандарты обеспечения информационной безопасности. Определяются основные компоненты защиты информации.

Информационная безопасность не является залогом безопасности вашей компании, информации и компьютерных систем. К сожалению, обеспечить надежную защиту "по взмаху волшебной палочки" нельзя. Но реализовать ее на должном уровне вполне реально, хотя концепции, лежащие в ее основе, не очень-то и просты.

Информационная безопасность - это система, позволяющая выявлять уязвимые места организации, опасности, угрожающие ей, и справляться с ними. К сожалению, известно много примеров, когда продукты, считающиеся "лекарством на все случаи жизни", на самом деле уводили в сторону от выработки надлежащих способов эффективной защиты. Свою лепту вносили их производители, заявляющие о том, что именно их продукт решает все проблемы безопасности.

Понятие об информационной безопасности

В онлайновом словаре Мерриама_Вебстера (Merriam-Webster) (http://www.m-w.com/) дается следующее определение информации:

- сведения, полученные при исследовании, изучении или обучении;
- известия, новости, факты, данные;
- команды или символы представления данных (в системах связи или в компьютере);
- знания (сообщения, экспериментальные данные, изображения), меняющие концепцию, полученную в результате физического или умственного опыта.

Безопасность определяется следующим образом: свобода от опасности, сохранность; свобода от страха или беспокойства.

Если мы объединим эти два понятия вместе, то получим определение информационной безопасности - меры, принятые для предотвращения несанкционированного использования, злоупотребления, изменения сведений, фактов, данных или аппаратных средств либо отказа в доступе к ним.

Как следует из определения, информационная безопасность не обеспечивает абсолютную защиту. Вы построите самую прочную крепость в мире - и тут

же появится кто-то с еще более мощным тараном. Информационная безопасность - это предупредительные действия, которые позволяют защитить информацию и оборудование от угроз и использования их уязвимых мест.

Внимание!

Если вы собираетесь работать системным администратором или консультантом в системе обеспечения безопасности, не совершайте ошибку, думая, что секретной информации ничто не угрожает. Возможно, это самая серьезная ошибка на сегодняшний день.

Краткая история безопасности

Способы защиты информации и других ресурсов постоянно меняются, как меняется наше общество и технологии. Очень важно понять это, чтобы выработать правильный подход к обеспечению безопасности. Поэтому давайте немного познакомимся с ее историей, чтобы избежать повторения прошлых ошибок.

Физическая безопасность

На заре цивилизации ценные сведения сохранялись в материальной форме: вырезались на каменных табличках, позже записывались на бумагу. Для их защиты использовались такие же материальные объекты: стены, рвы и охрана.

Примечание

Важную или секретную информацию старались не сохранять на твердых носителях, наверное поэтому до нас дошло так мало записей алхимиков. Они не обсуждали свои секреты ни с кем, кроме избранных учеников, ведь знание - это сила. Наверное, это и было самой лучшей защитой. Сунь Цзы говорил: "Секрет, который знает больше чем один, - уже не секрет".

Информация передавалась обычно с посыльным и в сопровождении охраны. И эти меры себя оправдывали, поскольку единственным способом получения информации было ее похищение.

Защита информации в процессе передачи

К сожалению, физическая защита имела один недостаток. При захвате сообщения враги узнавали все, что было написано в нем. Еще Юлий Цезарь принял решение защищать ценные сведения в процессе передачи. Он изобрел шифр Цезаря. Этот шифр позволял посылать сообщения, которые никто не мог прочитать в случае перехвата.

Данная концепция получила свое развитие во время Второй мировой войны. Германия использовала машину под названием Enigma (рис. 1.1) для шифрования сообщений, посылаемых воинским частям.

Рис. 1.1. Шифровальная машина Enigma

Немцы считали, что машину Enigma практически невозможно было взломать. Ее действительно было бы очень трудно взломать - если бы не ошибки операторов, позволившие союзникам прочитать некоторые сообщения. В военном деле обычно применяли кодовые слова для обозначения географических пунктов и боевых подразделений. Япония заменяла названия кодовыми словами, так что понять их сообщения было очень сложно даже после взлома шифровального кода.

Вопрос к эксперту

Вопрос.Какое самое слабое звено в безопасности?

Ответ. Прежде всего, люди. Хорошим примером является Германия во Второй мировой войне. Операторы машины Enigma использовали стандартные сокращения для облегчения своей работы. Нельзя не вспомнить разведчиков бывшего Советского Союза и их одноразовые ключи (об этом пойдет речь дальше). В любой системе безопасности самое слабое звено - это человеческие слабости.

Во время подготовки к битве за Мидуэй американские дешифровщики предприняли попытку идентификации цели, которая была упомянута в японских шифровках как "AF". Они открытым текстом передали сообщение о нехватке воды на острове Мидуэй. После перехвата этого сообщения японцы в своей шифровке известили о том, что на "AF" нет воды. Так американцы поняли, что "AF" на самом деле означает "Мидуэй".

Шифровались не только военные донесения. Для защиты от прослушивания в американских воинских частях использовали радистов из народа навахо, которые вели переговоры на родном языке. При перехвате радиосообщений противник не мог понять их содержание.

После Второй мировой войны Советский Союз использовал одноразовые ключи при передаче информации разведчиками. Эти ключи на самом деле представляли собой бумажные блокноты со случайным расположением цифр на каждой странице. Каждая страница предназначалась только для одного сообщения. Такая схема шифрования могла бы стать действительно уникальной, однако разовые ключи использовались не по одному разу, благодаря чему некоторые сообщения удалось расшифровать.

Защита излучения

Если не считать ошибок при использовании шифровальных систем, сложный шифр очень трудно взломать. Поэтому шел постоянный поиск других способов перехвата информации, передаваемой в зашифрованном виде.

В 1950 г. было установлено, что доступ к сообщениям возможен посредством просмотра электронных сигналов, возникающих при их передаче по телефонным линиям (рис. 1.2).

Работа любых электронных систем сопровождается излучением, в том числе телетайпов и блоков шифрования, используемых для передачи зашифрованных сообщений. Блок шифрования посылает зашифрованное сообщение по телефонной линии, а вместе с ним передается и электрический сигнал от исходного сообщения. Следовательно, при наличии хорошей аппаратуры исходное сообщение можно восстановить.

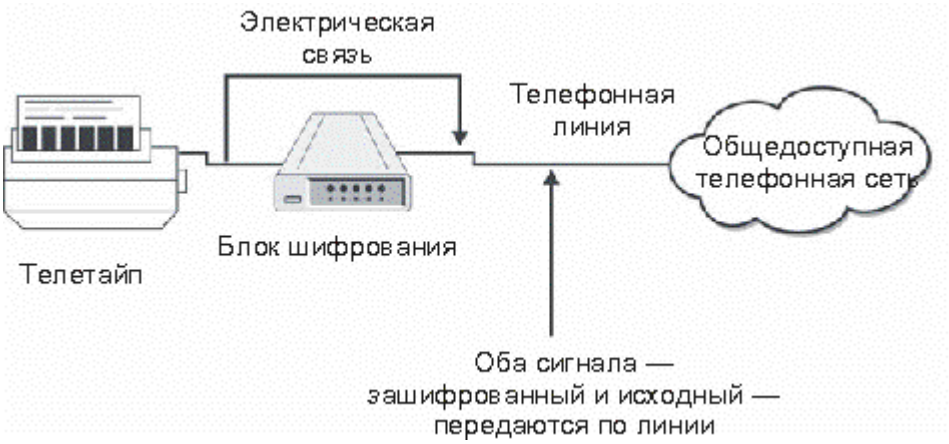

Рис. 1.2. Электронные сигналы "обходят" шифрование

Проблема защиты излучения привела к созданию в Соединенных Штатах Америки программы "TEMPEST". Эта программа разработала стандарты на электрическое излучение компьютерных систем, используемых в секретных организациях. Целью программы было уменьшение уровня излучения, которое могло бы быть использовано для сбора информации.

Примечание

Система "TEMPEST" играет важную роль в некоторых секретных правительственных программах. У коммерческих организаций тоже есть все основания для беспокойства, но вряд ли оно настолько велико, что заставит их раскошелиться на использование в своей работе системы захвата компьютерного излучения.

Защита компьютера

При передаче сообщений по телеграфу достаточно было обеспечить защиту коммуникаций и излучения. Затем появились компьютеры, на которые были перенесены в электронном формате информационные ресурсы организаций. Спустя какое-то время работать на компьютерах стало проще, и многие пользователи научились общаться с ними в режиме интерактивного диалога. К информации теперь мог обратиться любой пользователь, вошедший в систему. Возникла потребность в защите компьютеров.

В начале 70-х гг. XX века Дэвид Белл и Леонард Ла Падула разработали модель безопасности для операций, производимых на компьютере. Эта модель базировалась на правительственной концепции уровней классификации информации (несекретная, конфиденциальная, секретная, совершенно секретная) и уровней допуска. Если человек (субъект) имел уровень допуска выше, чем уровень файла (объекта) по классификации, то он получал доступ к файлу, в противном случае доступ отклонялся. Эта концепция нашла свою реализацию в стандарте 5200.28 "Trusted Computing System Evaluation Criteria" (TCSEC) ("Критерий оценки безопасности

компьютерных систем"), разработанном в 1983 г. Министерством обороны США. Из-за цвета обложки он получил название "Оранжевая книга". "Оранжевая книга" ранжировала компьютерные системы в соответствии со следующей шкалой.

D Минимальная защита (ненормируемая)

C1 Защита по усмотрению

C2 Контролируемая защита доступа

B1 Защита с метками безопасности

B2 Структурированная защита

B3 Защита доменов

A1 Проверяемая разработка

"Оранжевая книга" определяла для каждого раздела функциональные требования и требования гарантированности. Система должна была удовлетворять этим требованиям, чтобы соответствовать определенному уровню сертификации.

Выполнение требований гарантированности для большинства сертификатов безопасности отнимало много времени и стоило больших денег. В результате очень мало систем было сертифицировано выше, чем уровень C2 (на самом деле только одна система за все время была сертифицирована по уровню A1 - Honeywell SCOMP). За то время, которое требовалось системам для прохождения сертификации, они успевали устареть.

При составлении других критериев были сделаны попытки разделить функциональные требования и требования гарантированности. Эти разработки вошли в "Зеленую книгу" Германии в 1989 г., в "Критерии Канады" в 1990 г., "Критерии оценки безопасности информационных технологий" (ITSEC) в 1991 г. и в "Федеральные критерии" (известные как Common Criteria - "Общие критерии") в 1992 г. Каждый стандарт предлагал свой способ сертификации безопасности компьютерных систем. ITSEC и Common Criteria продвинулись дальше остальных, оставив функциональные требования фактически не определенными.

Современная концепция безопасности воплощена в "Общих критериях". Главная идея сосредоточена в так называемых профилях защиты, определяющих различные среды безопасности, в которые может быть помещена компьютерная система. Продукты проходят оценку на соответствие этим профилям и сертифицируются. При покупке системы

организация имеет возможность выбрать профиль, наиболее полно соответствующий ее потребностям, и подобрать продукты, сертифицированные по этому профилю. Сертификат продукта включает также уровень доверия, т. е. уровень секретности, заложенный оценщиками, соответствующий профилю функциональных возможностей.

Технологии компьютерных систем слишком быстро развиваются по сравнению с программой сертификации. Возникают новые версии операционных систем и аппаратных средств и находят свои рынки сбыта еще до того, как более старшие версии и системы проходят сертификацию.

Примечание

"Федеральные критерии" существуют до сих пор, и некоторые приложения требуют сертифицированных систем для своей работы.

Защита сети

Одна из проблем, связанных с критериями оценки безопасности систем, заключалась в недостаточном понимании механизмов работы в сети. При объединении компьютеров к старым проблемам безопасности добавляются новые. Да, мы имеем средства связи, но при этом локальных сетей гораздо больше, чем глобальных. Скорости передачи стали выше, появилось множество линий общего пользования. Шифровальные блоки иногда отказываются работать. Существует излучение от проводки, проходящей по всему зданию. И, наконец, появились многочисленные пользователи, имеющие доступ к системам. В "Оранжевой книге" не рассматривались проблемы, возникающие при объединении компьютеров в общую сеть. Сложившееся положение таково, что наличие сети лишает законной силы сертификат "Оранжевой книги". Ответной мерой стало появление в 1987 г. TNI (Trusted Network Interpretation), или "Красной книги". В "Красной книге" сохранены все требования к безопасности из "Оранжевой книги", сделана попытка адресации сетевого пространства и создания концепции безопасности сети. К сожалению, и "Красная книга" связывала функциональность с гарантированностью. Лишь некоторые системы прошли оценку по TNI, и ни одна из них не имела коммерческого успеха.

В наши дни проблемы стали еще серьезнее. Организации стали использовать беспроводные сети, появления которых "Красная книга" не могла предвидеть. Для беспроводных сетей сертификат "Красной книги" считается устаревшим.

Защита информации

Итак, куда же нас привела история? Создается впечатление, что ни одно из решений не устраняет проблем безопасности. В реальной жизни надежная

защита - это объединение всех способов защиты (рис. 1.3). Надежная физическая защита необходима для обеспечения сохранности материальных активов - бумажных носителей и систем. Защита коммуникаций (COMSEC) отвечает за безопасность при передаче информации. Защита излучения (EMSEC) необходима, если противник имеет мощную аппаратуру для чтения электронной эмиссии от компьютерных систем. Компьютерная безопасность (COMPUSEC) нужна для управления доступом в компьютерных системах, а безопасность сети (NETSEC) - для защиты локальных сетей. В совокупности все виды защиты обеспечивают информационную безопасность (INFOSEC).

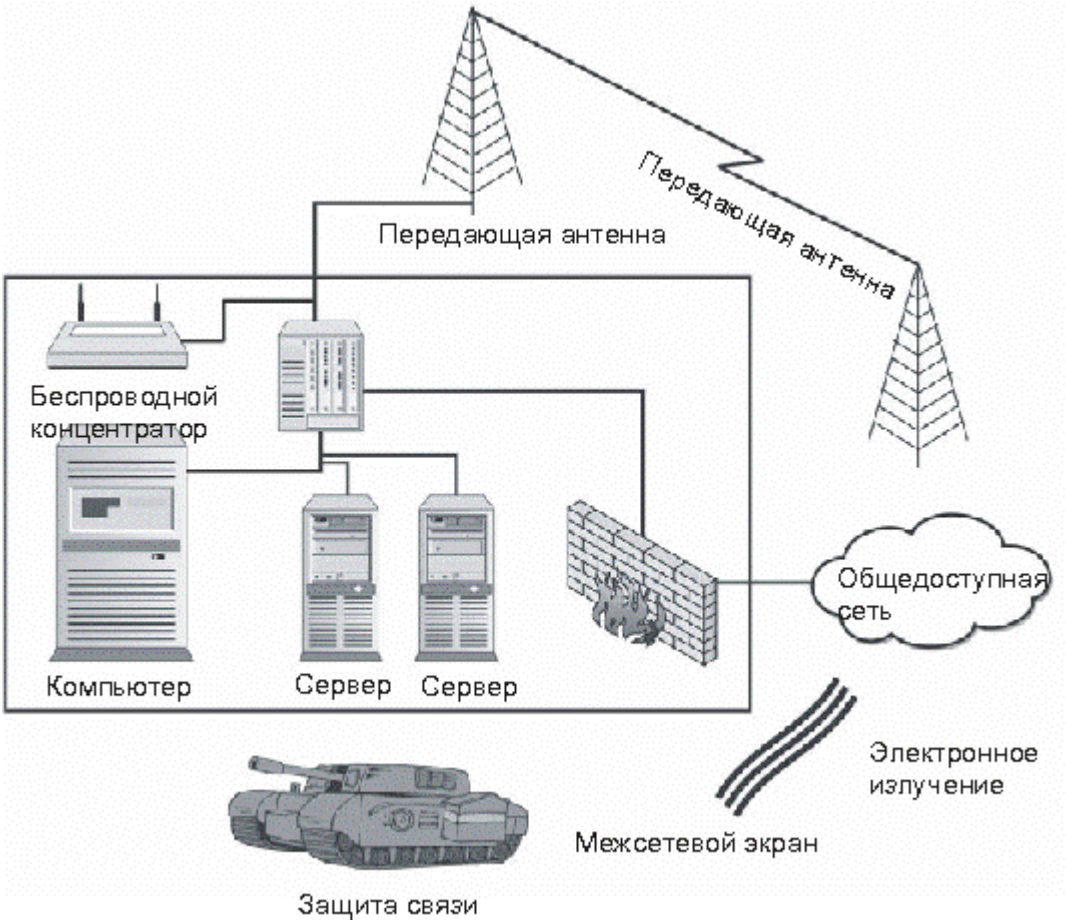

Рис. 1.3. Информационная безопасность включает множество аспектов безопасности

До настоящего времени не разработан процесс сертификации компьютерных систем, подтверждающий обеспечиваемую безопасность. Для большинства предлагаемых решений технологии слишком быстро ушли вперед. Лабораторией техники безопасности США (Underwriters Laboratory) была предложена новая концепция безопасности, согласно которой необходимо создать центр сертификации, удостоверяющий безопасность различных продуктов. Если совершено проникновение в систему, пользователи которой работали с несертифицированным продуктом, то это следует расценивать как халатное отношение к безопасности администраторов этой системы.

К сожалению, эта концепция создает две проблемы.

- Темп развития технологий ставит под сомнение тот факт, что центр представит самые лучшие сертифицированные продукты, прежде чем они станут устаревшими.
- Чрезвычайно трудно, почти невозможно доказать, будто что-то надежно защищено. Фактически центр сертификации должен опровергнуть тот факт, что систему можно взломать. Что делать, если завтра все существующие сертификаты устареют? Придется сертифицировать все системы заново?

Поскольку промышленность продолжает поиск новых решений, остается определить безопасность как лучшее, что можно сделать. Безопасность достигается через повседневную практику и постоянную бдительность

Вопросы для самопроверки

1. Программа, накладывающая ограничения на излучение компьютеров, называется _____.
2. Радисты, говорящие на языке навахо, использовались во время Второй мировой войны для обеспечения _____ безопасности.

Определение безопасности как процесса

Очевидно, что нельзя полагаться на один вид защиты для обеспечения безопасности информации. Не существует и единственного продукта, реализующего все необходимые способы защиты для компьютеров и сетей. К сожалению, многие разработчики претендуют на то, что только их продукт может справиться с этой задачей. На самом деле это не так. Для всесторонней защиты информационных ресурсов требуется множество различных продуктов. Об этом и пойдет речь в следующих разделах.

Антивирусное программное обеспечение

Антивирусное программное обеспечение является неотъемлемой частью надежной программы безопасности. При его правильной настройке значительно уменьшается риск воздействия вредоносных программ (хотя и не всегда - вспомните про вирус Melissa).

Но никакая антивирусная программа не защитит организацию от злоумышленника, использующего для входа в систему законную программу, или от легального пользователя, пытающегося получить несанкционированный доступ к файлам

Управление доступом

Любая компьютерная система в пределах организации ограничивает доступ к файлам, идентифицируя пользователя, который входит в систему. При

правильной настройке системы, при установке необходимых разрешений для легальных пользователей существует ограничение на использование файлов, к которым у них нет доступа. Однако система управления доступом не обеспечит защиту, если злоумышленник через уязвимые места получит доступ к файлам как администратор. Такое нападение будет считаться легальными действиями администратора.

Межсетевые экраны

Межсетевой экран (firewall) - это устройство управления доступом, защищающее внутренние сети от внешних атак. Оно устанавливается на границе между внешней и внутренней сетью. Правильно сконфигурированный межсетевой экран является важнейшим устройством защиты. Однако он не сможет предотвратить атаку через разрешенный канал связи. Например, при разрешении доступа к веб-серверу с внешней стороны и наличии слабого места в его программном обеспечении межсетевой экран пропустит эту атаку, поскольку открытое веб-соединение необходимо для работы сервера. Межсетевой экран не защитит от внутренних пользователей, поскольку они уже находятся внутри системы. Под внутреннего пользователя может замаскироваться злоумышленник. Рассмотрим организацию, имеющую беспроводные сети. При неправильной настройке внутренней беспроводной сети злоумышленник, сидя на стоянке для автомобилей, сможет перехватывать данные из этой сети, при этом его действия будут выглядеть как работа пользователя внутри системы. В этом случае межсетевой экран не поможет.

Смарт-карты

Аутентификация (установление подлинности) личности может быть выполнена при использовании трех вещей: того, что вы знаете, того, что вы имеете, или того, чем вы являетесь. Исторически для идентификации личности в компьютерных системах применялись пароли (то, что вы знаете). Но оказалось, что надеяться на пароли особо не следует. Пароль можно угадать, либо пользователь запишет его на клочке бумаги - и пароль узнают все. Решает эту проблему применение других методов аутентификации.

Для установления личности используются смарт-карты (они - то, что вы имеете), и таким образом уменьшается риск угадывания пароля. Однако если смарт-карта украдена, и это - единственная форма установления подлинности, то похититель сможет замаскироваться под легального пользователя компьютерной системы. Смарт-карты не смогут предотвратить атаку с использованием уязвимых мест, поскольку они рассчитаны на правильный вход пользователя в систему.

Еще одна проблема - это стоимость смарт-карт, ведь за каждую нужно заплатить от 50 до 100 долларов. Организации с большим количеством служащих потребуются серьезные затраты на оплату такой безопасности.

Биометрия

Биометрические системы - еще один механизм аутентификации (они - то, чем вы являетесь), значительно уменьшающий вероятность угадывания пароля. Существует множество биометрических сканеров для верификации следующего:

- отпечатков пальцев;
- сетчатки/радужной оболочки;
- отпечатков ладоней;
- конфигурации руки;
- конфигурации лица;
- голоса.

Каждый метод предполагает использование определенного устройства для идентификации человеческих характеристик. Обычно эти устройства довольно сложны, чтобы исключить попытки обмана. Например, при снятии отпечатков пальцев несколько раз проверяются температура и пульс. При использовании биометрии возникает множество проблем, включая стоимость развертывания считывающих устройств и нежелание сотрудников их использовать.

Внимание!

Перед развертыванием биометрической системы удостоверьтесь, что служащие организации согласны ее использовать. Не каждый захочет размещать свой глаз в лазерном луче для сканирования сетчатки!

Как и другие сильные опознавательные методы, биометрия эффективна в случае правильного входа в систему. Если злоумышленник найдет пути обхода биометрической системы, она не сможет обеспечить безопасность.

Обнаружение вторжения

Системы обнаружения вторжения (Intrusion Detection System, IDS) неоднократно рекламировались как полное решение проблемы безопасности. Нашим компьютерам больше не нужна защита, теперь легко определить, что в системе кем-то выполняются недозволенные действия, и остановить его! Многие IDS позиционировались на рынке как системы, способные остановить атаки до того, как они успешно осуществятся. Кроме того, появились новые системы - системы предотвращения вторжения (Intrusion Prevention System, IPS). Следует заметить, что никакая система обнаружения

вторжения не является устойчивой к ошибкам, она не заменит надежную программу безопасности или практику безопасности. С помощью этих систем нельзя выявить законных пользователей, пытающих получить несанкционированный доступ к информации.

Системы обнаружения вторжения с автоматической поддержкой защиты отдельных участков создают дополнительные проблемы. Представьте, что система IDS настроена на блокировку доступа с предполагаемых адресов нападения. В это время ваш клиент сгенерировал трафик, который по ошибке был идентифицирован системой как возможная атака. Не удивляйтесь потом, что этот клиент больше не захочет иметь с вами дело!

Управление политиками

Политики и управление ими - важные компоненты надежной программы безопасности. С их помощью организация получает сведения о системах, не соответствующих установленным политикам. Однако этот компонент не учитывает наличие уязвимых мест в системах или неправильную конфигурацию прикладного программного обеспечения, что может привести к успешному проникновению в систему. Управление политиками не гарантирует, что пользователи не будут пренебрежительно относиться к своим паролям или не передадут их злоумышленникам.

Сканирование на наличие уязвимых мест

Сканирование компьютерных систем на наличие уязвимых мест играет важную роль в программе безопасности. Оно позволит выявить потенциальные точки для вторжения и предпринять немедленные меры для повышения безопасности. Однако такое исследование не остановит легальных пользователей, выполняющих несанкционированный доступ к файлам, не обнаружит злоумышленников, которые уже проникли в систему через "прорехи" в конфигурации.

Шифрование

Шифрование - важнейший механизм защиты информации при передаче. С помощью шифрования файлов можно обеспечить также безопасность информации при хранении. Однако служащие организации должны иметь доступ к этим файлам, а система шифрования не сможет различить законных и незаконных пользователей, если они представят одинаковые ключи для алгоритма шифрования. Для обеспечения безопасности при шифровании необходим контроль за ключами шифрования и системой в целом.

Механизмы физической защиты

Физическая защита - единственный способ комплексной защиты компьютерных систем и информации. Ее можно выполнить относительно дешево. Для этого выройте яму глубиной 20 метров, поместите в нее важные системы и сверху залейте бетоном. Все будет в полной безопасности! К сожалению, появятся проблемы с сотрудниками, которым нужен доступ к компьютерам для нормальной работы.

Даже при наличии механизмов физической защиты, тщательно расставленных по своим местам, вам придется дать пользователям доступ к системе - и ей скоро придет конец! Физическая защита не предотвратит атаку с использованием легального доступа или сетевую атаку.

Проект 1. Проверка сертификатов компьютерной безопасности

В этом проекте мы покажем, что сертификаты систем компьютерной безопасности не удовлетворяют потребностям индустрии безопасности. Оценим существующие операционные системы в соответствии с критериями "Оранжевой книги"

Шаг за шагом

1. Определите, какие операционные системы используются в вашем офисе. Выберите одну из них.
2. Скопируйте "Оранжевую книгу" с веб-сайта по адресу http://www.radium.ncsc.mil/tpep/library/rainbow/.
3. Начните с проверки функциональных требований раздела С "Оранжевой книги". Они находятся под заголовком "Политики безопасности" и "Идентифицируемость". На этом этапе игнорируйте требования гарантированности и документирования.
4. Определите, отвечает ли данная система требованиям раздела С. Если это так, то переходите к разделам В и А.
5. После определения функционального уровня системы проверьте требования гарантированности и документирования для этого же уровня. Выполняются ли эти требования?

Выводы

В зависимости от типа операционные системы практически всегда имеют функциональность уровня С1. Уровень С2 основывается на требовании безопасности повторного использования объекта, и большинство коммерческих операционных систем отвечают требованиям функциональности этого уровня. Эти системы не имеют функциональности, соответствующей уровню В.

Требования гарантированности и документирования даже для уровня С1 вряд ли можно встретить в стандартной документации к программному

обеспечению. Удивляет вас теперь тот факт, что очень маленькое количество систем смогли пройти оценку и сертификацию?

Контрольные вопросы

1. Что такое информационная безопасность?
2. Какие компоненты входят в информационную безопасность?
3. Почему возникла необходимость в защите компьютеров?
4. Почему организации сталкиваются с проблемами при обеспечении информационной безопасности?
5. Являются ли системы, сертифицированные по уровню C2 правительства США, самыми защищенными?
6. Почему безопасность - это процесс, а не конечный продукт?
7. Сколько систем получили сертификат по уровню A1?
8. Почему "Оранжевая книга" утратила свою силу?
9. Была ли операционная система Microsoft Windows NT сертифицирована по уровню C2 "Оранжевой книги"?
10. Что значит TNI?
11. Почему физическая защита не может гарантировать безопасность?
12. Полагаются ли системы управления доступом на другие системы?
13. От какого нападения защищают межсетевые экраны?
14. Какие три вещи используются для установления подлинности личности?
15. Назовите два типа биометрических систем.