Информационная безопасность. Учет понятия об информационной безопасности при создании комплексных информационных объектов в виде веб-страниц

От степени безопасности информационных технологий в настоящее время зависит благополучие, а порой и жизнь многих людей.

Под информационной безопасностью понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.

На практике важнейшими являются три аспекта информационной безопасности:

- ***доступность*** (возможность за разумное время получить требуемую информационную услугу);
- ***целостность*** (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- ***конфиденциальность*** (защита от несанкционированного прочтения).

Основные угрозы информационной безопасности

Нарушения доступности, целостности и конфиденциальности информации могут быть вызваны различными опасными воздействиями на информационные компьютерные системы.

Современная информационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя.

Основные угрозы информационной безопасности

Компоненты автоматизированной информационной системы можно разбить на следующие группы:

- ***аппаратные средства*** - компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства - дисководы, принтеры, контроллеры, кабели, линии связи и т.д.);
- ***программное обеспечение*** - приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.;
- ***данные*** - хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
- ***персонал*** - обслуживающий персонал и пользователи.

Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные.

Причинами ***случайных воздействий*** при эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

***Преднамеренные воздействия* - это целенаправленные действия нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник.**

***Действия нарушителя могут быть обусловлены разными мотивами*:**

- недовольством служащего своей карьерой;
- взяткой;
- любопытством;
- конкурентной борьбой;
- стремлением самоутвердиться любой ценой.
- Можно составить гипотетическую модель потенциального нарушителя:
- квалификация нарушителя на уровне разработчика данной системы;
- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- нарушителю известна информация о принципах работы системы;
- нарушитель выбирает наиболее слабое звено в защите.

Наиболее распространенным и многообразным видом компьютерных нарушений является несанкционированный доступ(НСД).

НСД использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке.

Классификация каналов НСД:

- через человека:
- хищение носителей информации;
- чтение информации с экрана или клавиатуры;
- чтение информации из распечатки.
- Через программу:
- перехват паролей;
- дешифровка зашифрованной информации;
- копирование информации с носителя.
- Через аппаратуру:
- подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т.д.

Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена.

Компьютерные сети характерны тем, что против них предпринимают так называемые удаленные атаки.

Обеспечение информационной безопасности

Формирование режима информационной безопасности - проблема комплексная.

Меры по ее решению можно подразделить на пять уровней:

- ***законодательный*** ***(законы, нормативные акты, стандарты и т.п.);***
- ***морально-этический*** ***(всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации);***
- ***административный*** ***(действия общего характера, предпринимаемые руководством организации);***
- ***физический*** ***(механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей);***
- ***аппаратно-программный*** ***(электронные устройства и специальные программы защиты информации).***

Единая совокупность всех мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Надежная система защиты должна соответствовать следующим принципам:

- Стоимость средств защиты должна быть меньше, чем размеры возможного ущерба.
- Каждый пользователь должен иметь минимальный набор привилегий, необходимый для работы.
- Защита тем более эффективна, чем проще пользователю с ней работать.
- Возможность отключения в экстренных случаях.
- Специалисты, имеющие отношение к системе защиты должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать.

Аппаратно-программные средства защиты информации

Несмотря на то, что современные ОС для персональных компьютеров имеют собственные подсистемы защиты, актуальность создания дополнительных средств защиты сохраняется.

Дело в том, что большинство систем не способны защитить данные, находящиеся за их пределами, например при сетевом информационном обмене.

Аппаратно-программные средства защиты информации можно разбить на пять групп:

- Системы идентификации (распознавания) и аутентификации (проверки подлинности) пользователей.
- Системы шифрования дисковых данных.
- Системы шифрования данных, передаваемых по сетям.
- Системы аутентификации электронных данных.
- Средства управления криптографическими ключами.

1. Системы идентификации и аутентификации пользователей

При построении этих систем возникает проблема выбора информации, на основе которой осуществляются процедуры идентификации и аутентификации пользователя. Можно выделить следующие **типы**:

- секретная информация, которой обладает пользователь (пароль, секретный ключ, персональный идентификатор и т.п.);
- физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т.п.).

Системы, основанные на первом типе информации, считаются ***традиционными***. Системы, использующие второй тип информации, называют ***биометрическими***.

2. Системы шифрования дисковых данных

Чтобы сделать информацию бесполезной для противника, используется совокупность методов преобразования данных, называемая криптографией.

Системы шифрования могут осуществлять криптографические преобразования данных на уровне файлов или на уровне дисков.

Другим классификационным признаком систем шифрования дисковых данных является способ их функционирования.

2. Системы шифрования дисковых данных

По способу функционирования системы шифрования дисковых данных делят на два класса:

- системы "прозрачного" шифрования;
- системы, специально вызываемые для осуществления шифрования.

В системах прозрачного шифрования (шифрования "на лету") криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя.

Системы второго класса обычно представляют собой утилиты, которые необходимо специально вызывать для выполнения шифрования. К ним относятся, например, архиваторы со встроенными средствами парольной защиты.

3. Системы шифрования данных, передаваемых по сетям

Различают два основных способа шифрования:

канальное шифрование и оконечное (абонентское) шифрование.

В случае ***канального шифрования*** защищается вся информация, передаваемая по каналу связи, включая служебную.

Оконечное (абонентское) шифрование позволяет обеспечить конфиденциальность данных, передаваемых между двумя абонентами.

4. Системы аутентификации электронных данных

При обмене данными по сетям возникает проблема аутентификации автора документа и самого документа, т.е. установление подлинности автора и проверка отсутствия изменений в полученном документе. Для аутентификации данных применяют код аутентификации сообщения (имитовставку) или электронную подпись.

Имитовставка вырабатывается из открытых данных посредством специального преобразования шифрования с использованием секретного ключа и передается по каналу связи в конце зашифрованных данных.

Электронная цифровая подпись представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом.

5. Средства управления криптографическими ключами

Безопасность любой криптосистемы определяется используемыми криптографическими ключами. В случае ненадежного управления ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в системе или сети.

Различают следующие виды функций управления ключами:

- генерация,
- хранение,
- распределение ключей.

Способы ***генерации ключей*** для симметричных и асимметричных криптосистем различны. Для генерации ключей симметричных криптосистем используются аппаратные и программные средства генерации случайных чисел. Генерация ключей для асимметричных криптосистем более сложна, так как ключи должны обладать определенными математическими свойствами.

Функция ***хранения*** предполагает организацию безопасного хранения, учета и удаления ключевой информации. Для обеспечения безопасного хранения ключей применяют их шифрование с помощью других ключей. Такой подход приводит к концепции иерархии ключей.

Распределение - самый ответственный процесс в управлении ключами. Этот процесс должен гарантировать скрытность распределяемых ключей, а также быть оперативным и точным. Между пользователями сети ключи распределяют двумя способами:

- с помощью прямого обмена сеансовыми ключами;
- используя один или несколько центров распределения ключей.

Что учесть при обеспечении информационной безопасности сайта

Способов защитить свой сайт:

- контроль доступа.
- обеспечить защиту от DDoS-атак;
- подключить SSL-сертификат;
- использовать надёжный хостинг;
- использовать безопасные плагины/библиотеки/фреймворки/CMS (далее – «сторонние модули»);
- применять существующие техники защиты от SQL-инъекций и XSS-атак;
- обеспечить ведение журнала веб-сайта и мониторинг событий безопасности;
- производить регулярное резервное копирование веб-сайта и всех важных данных;
- использовать надёжные и сложные пароли, а также защиту от перебора паролей;
- в случае наличия административной панели, с помощью которой происходит управление содержимым веб-сайта, необходимо изменить стандартный адрес входа и обеспечить