Лекционный материал по курсу «Информационная безопасность».

1. Методы взлома компьютерных систем. Этапы осуществления атаки.

Все попытки взлома защиты компьютерных систем разделяют на три группы:

1.Атаки на уровне операционной системы

Соблюдение адекватной политики безопасности является значительно более трудной задачей для данного уровня, т.к. внутренняя структура современных операционных систем чрезвычайно сложна. От архитектуры и конфигурации конкретной операционной системы, являющейся объектом этой атаки, зависит успех реализации алгоритма атаки.

Атаки, которым может быть подвергнута практически любая операционная система:

- кража пароля;
- получение пароля из файла, в котором этот пароль был сохранен пользователем;
- кража внешнего носителя парольной информации (дискеты или электронного ключа, на которых хранится пароль пользователя, предназначенный для входа в операционную систему);
- полный перебор всех возможных вариантов пароля;
- подбор пароля по частоте встречаемости символов, с помощью словарей наиболее часто применяемых паролей;
- подмена динамически загружаемой библиотеки, используемой системными программами, или изменение переменных среды, описывающих путь к таким библиотекам;

- модификация кода или данных подсистемы защиты самой операционной системы;

2. Атаки на уровне систем управления базами данных.

Защищать операционную систему гораздо сложнее в отличие от СУБД, но чтобы получить доступ к файлам СУБД, большинство хакеров делают это с помощью средств ОС.

Существуют два специфических сценария атаки на СУБД, для защиты от которых требуется применять специальные методы.

В первом случае результаты арифметических операций над числовыми полями СУБД округляются в меньшую сторону, а разница суммируется в некоторой другой записи СУБД.

Во втором случае хакер получает доступ к полям записей СУБД, для которых доступной является только статистическая информация. Идея хакерской атаки на СУБД — так сформулировать запрос, чтобы множество записей, для которого собирается статистика, состояло только из одной записи.

3. Атаки на уровне сетевого программного обеспечения.

СПО является наиболее уязвимым, потому что канал связи, по которому передаются сообщения, чаше всего не защищен.

На уровне СПО возможны следующие атаки:

- **сегмента локальной сети** (в пределах одного и того же сегмента локальной сети любой подключенный к нему компьютер в состоянии принимать сообщения, адресованные другим компьютерам сегмента, а следовательно, если компьютер хакера подсоединен к некоторому сегменту локальной сети, то ему становится доступен весь информационный обмен между компьютерами этого сегмента);
- **перехват сообщений на** маршрутизаторе (если хакер имеет привилегированный доступ к сетевому маршрутизатору, то он получает возможность выборочного перехвата всех сообщений, проходящие через этот маршрутизатор);
- **создание ложного** маршрутизатора (путем отправки в сеть сообщений специального вида хакер добивается, чтобы его компьютер стал

маршрутизатором сети, после чего получает доступ ко всем проходящим через него сообщениям);

- **навязывание сообщений** (отправляя в сеть сообщения с ложным обратным сетевым адресом, хакер переключает на свой компьютер уже установленные сетевые соединения и в результате получает права пользователей, чьи соединения обманным путем были переключены на компьютер хакера).

2. Классификация компьютерных атак и систем их обнаружения.

Эффективная защита от потенциальных сетевых атак невозможна без их детальной классификации. В настоящее время известно большое количество различных типов классификационных признаков. В качестве таких признаков может быть выбрано, разделение на пассивные и активные, внешние и внутренние атаки, умышленные и неумышленные и т.д.

Бывают атаки:

- удаленное проникновение (от англ. remote penetration) — это тип атак, которые позволяют реализовать удаленное управление компьютером через сеть (например, атаки с использованием программ NetBus или BackOrifice);
- локальное проникновение (от англ. local penetration) — это тип атак , которые приводят к получению несанкционированного доступа к узлу, на который они направлены; примером такой атаки является атака с использованием программы GetAdmin;
- удаленный отказ в обслуживании (от англ. remote denial of service) — тип атак , которые позволяют нарушить функционирование системы в рамках глобальной сети; пример такой атаки — Teardrop или trinOO;
- локальный отказ в обслуживании (от англ. local denial of service) — тип атак, позволяющих нарушить функционирование системы в рамках локальной сети. В качестве примера такой атаки можно привести внедрение и запуск враждебной программы, которая загружает центральный процессор бесконечным циклом, что приводит к невозможности обработки запросов других приложений;

- атак и с использованием сетевых сканеров (от англ. network scanners) — это тип атак, основанных на использовании сетевых сканеров — программ, которые анализируют топологию сети и обнаруживают сервисы, доступные для атак и; пример: атак а с использованием утилиты nmap;
- атак и с использованием сканеров уязвимостей (от англ. vulnerability scanners) — тип атак, основанных на использовании сканеров уязвимостей — программ, осуществляющих поиск уязвимостей на узлах сети, которые в дальнейшем могут быть применены для реализации сетевых атак; примерами сетевых сканеров могут служить систем ы SATAN и Shadow Security Scanner;
- атак и с использованием взломщиков паролей (от англ. password crackers) — это тип атак, которые основаны на использовании взломщиков паролей — программ, подбирающих пароли пользователей; например, программа LOphtCrack для ОС Windows или программа Crack для ОС Unix;
- атак и с использованием анализаторов протоколов (от англ. sniffers) — это тип атак, основанных на использовании анализаторов протоколов — программах, "прослушивающих сетевой трафик. С их помощью можно автоматизировать поиск в сетевом трафике такой информации, как идентификаторы и пароли пользователей, информацию о кредитных картах и т. д. Примерами анализаторов сетевых протоколов являются программы Microsoft Network Monitor, NetXRay компании Network Associates или Lan Explorer.

3. Понятия: безопасность информации, цели обеспечения безопасности, целостность, готовность, конфиденциальность.

Информационная безопасность — это *состояние* защищённости информационной среды. *Защита информации* представляет собой *деятельность* по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть *процесс*, направленный на достижение этого состояния.

Безопасность информации — состояние защищенности информации, при котором обеспечиваются её конфиденциальность, доступность и целостность.

Цели обеспечения информационной безопасности.

Целостность информации — это условие того, что данные не были изменены при выполнении любой операции над ними, будь то передача, хранение или представление.

Конфиденциальность информации — принцип аудита, заключающийся в том, что аудиторы обязаны обеспечивать сохранность документов, получаемых или составляемых ими в ходе аудиторской деятельности, и не вправе передавать эти документы или их копии каким бы то ни было третьим лицам, либо разглашать устно содержащиеся в них сведения без согласия собственника экономического субъекта, за исключением случаев, предусмотренных законодательными актами.

Готовность информации – возможность доступа к информации с использованием соответствующих информационных технологий всегда, когда в ней возникает необходимость.

4. Понятия: информация, ценность информации, важность информации.

Информация (от лат. *informatio* — осведомление, разъяснение, изложение) - это доступная, сохраняемая или передаваемая группа данных, структурированная необходимым, для получения знания, образом. В узком смысле этого слова — сведения независимо от формы их представления.

Можно выделить 3 три вида ценности информации:

1. Информация обладает рыночной стоимостью сама по себе. Например, ноу-хау, изобретение, база клиентов и т.п.
2. Информация влияет на поведение людей, систем, процессов и ее стоимость вычисляется как разница в стоимости поведения до и после.

3. Информация снижает неопределенность, которая присуща любым бизнес-решениям, имеющим экономические последствия. Иными словами, мы должны измерить стоимость снижения неопределенности.

5. Классификация видов угроз.

Выделяют следующие компьютерные угрозы:

1. **семантическая угроза**, обеспечивающая добывание фактографической и индексно-ссылочной информации путем поиска, сбора и анализа структурируемой и неструктурируемой информации из общедоступных ресурсов или конфиденциальных источников компьютерных систем и сетей, а также путем семантической (аналитической) обработки полученных и накопленных массивов сведений и документов в целях создания специальных информационных массивов;

2. **алгоритмическая угроза** с использованием программно-аппаратных закладок и недекларированных возможностей, обеспечивающая добывание данных путем использования заранее внедренных изготовителем программно-аппаратных закладок, ошибок и недекларированных возможностей компьютерных систем и сетей;

3. **вирусная угроза**, обеспечивающая добывание данных путем внедрения и применения вредоносных программ в уже эксплуатируемые программные комплексы и системы для перехвата управления компьютерными системами;

4. **разграничительная угроза**, обеспечивающая добывание информации из отдельных (локальных) компьютерных систем, возможно и не входящих в состав сети, на основе преодоления средств разграничения доступа, а также реализация несанкционированного доступа при физическом доступе к компьютеру или компьютерным носителям информации;

5. **сетевая угроза**, обеспечивающая добывание данных из компьютерных сетей, путем реализации зондирования сети, инвентаризации и анализа уязвимостей сетевых ресурсов и последующего удаленного доступа к информации путем использования выявленных уязвимостей систем и средств

сетевой защиты ресурсов, а также блокирование доступа к ним, модификация, перехват управления либо маскирование своих действий;

6. **потоковая угроза**, обеспечивающая добывание информации и данных путем перехвата, обработки и анализа сетевого трафика (систем связи) и выявления структур компьютерных сетей и их технических параметров;

7. **аппаратная угроза**, обеспечивающая добывание информации и данных путем обработки сведений, получения аппаратуры, оборудования, модулей и их анализа, испытания для выявления их технических характеристик и возможностей;

8. **форматная угроза**, обеспечивающая добывание информации и сведений путем "вертикальной" обработки, фильтрации, декодирования и других преобразований форматов (представления, передачи и хранения) добытых данных в сведения, а затем в информацию для последующего ее наилучшего представления пользователям;

9. **пользовательская угроза**, обеспечивающая добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем обеспечения им доступа к информации, циркулирующей в специально созданной легендируемой (заманивающей) информационной инфраструктуре (приманка).

6. Разрушающие программные средства. Компьютерный вирус. Как он работает.

Класс разрушающих программных средств (РПС) составляют компьютерные вирусы, троянские кони и средства проникновения в удаленные системы через локальные и глобальные сети.

Компьютерный вирус — суть его сводится к тому, что программы приобретают свойства, присущие живым организмам, причем самые неотъемлемые – они рождаются, размножаются, умирают. Главное условие существования вирусов – универсальная интерпретация информации в

вычислительных системах. Вирус в процессе заражения программы может интерпретировать ее как данные, а в процессе выполнения как исполняемый код.

7. Классификация компьютерных вирусов.

Вирусы можно разделить на:

1.безвредные, никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате распространения);
2. неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;
3. опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;
4. очень опасные, в алгоритм работы, которых заведомо заложены процедуры, могущие привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.

Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как проникновение его в компьютер может вызвать непредсказуемые и порой катастрофические последствия.

8. Признаки заражения компьютера вирусом. Методы обнаружения и обезвреживания вируса.

- вывод на экран монитора компьютера неожиданных сообщений или изображений, не запланированных действиями пользователя или действиями программ работающих в данный момент;
-подача произвольных звуковых сигналов;
- произвольный запуск программ;
- сообщение сетевого экрана, о несанкционированном обращении незнакомых программ к ресурсам в сети;
- компьютер часто зависает, присутствуют постоянные сбои при работе программ;
- компьютер медленно работает при запуске некоторых программ;

- компьютер зависает на несколько секунд, потом работа продолжается в обычном режиме;
- операционная система загружается долго или вообще не грузится;
- искажается информация в некоторых файлах или каталогах;
- неожиданно появляются файлы или каталоги со странными именами;
- компьютер часто обращается к жесткому диску, хотя не какие программы не запускались и в данный момент не функционируют;
- интернет браузер часто зависает, самостоятельно изменяется стартовая страница.

Антивирусная защита.

- пользуйтесь самыми последними разработками в области компьютерной антивирусной защиты;
- регулярно обновляйте антивирусные базы;
- регулярно устанавливайте критические обновления для ваших программ и операционной системы;
- пользуйтесь сетевым экраном;
- внимательно изучайте обратный адрес отправителя и другие данные почтового сообщения, прежде, чем его открыть и прочитать;
- некогда не открывайте письма, присланные незнакомыми людьми;
- старайтесь избегать сайтов с пиратским программным обеспечением;
- используйте для путешествий по Интернету малораспространенные браузеры;
- старайтесь работать на компьютере в ограниченной учетной записи, а не под «администратором»;
- не открывайте полный доступ к папкам на вашем компьютере;
- не устанавливайте на компьютер сомнительные программы;
- не устанавливайте на компьютер программы из сомнительных источников;
- делайте как можно чаще резервные копии важных данных на внешние носители информации;
- разбейте ваш жесткий диск на логические диски, чтобы операционная система была отдельно размещена от важной информации и документов пользователей.

9. Программы обнаружения и защиты от вируса.

Основным средством борьбы с вирусами были и остаются антивирусные программы.

Сегодня используется несколько основополагающих методик обнаружения и защиты от вирусов:

1. сканирование;
2. эвристический анализ;
3. использование антивирусных мониторов;
4. обнаружение изменений.

Кроме того, практически все антивирусные программы обеспечивают автоматическое восстановление зараженных программ и загрузочных секторов.

Сканирование.

Самая простая методика поиска вирусов заключается в том, что антивирусная программа последовательно просматривает проверяемые файлы в поиске сигнатур известных вирусов. Под сигнатурой понимается уникальная последовательность байт, принадлежащая вирусу, и не встречающаяся в других программах.

Антивирусные программы-сканеры способны найти только уже известные и изученные вирусы, для которых была определена сигнатура.

Для шифрующихся и полиморфных вирусов, способных полностью изменять свой код при заражении новой программы или загрузочного сектора, невозможно выделить сигнатуру. Поэтому простые антивирусные программы-сканеры не могут обнаружить полиморфные вирусы.

Эвристический анализ.

Эвристический анализ позволяет обнаруживать ранее неизвестные вирусы, причем для этого не надо предварительно собирать данные о файловой системе.

Антивирусные программы, реализующие метод эвристического анализа, проверяют программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для вирусов. Эвристический анализатор может обнаружить, например, что проверяемая программа устанавливает

резидентный модуль в памяти или записывает данные в исполнимый файл программы.

Когда антивирус обнаруживает зараженный файл, он обычно выводит сообщение на экране монитора и делает запись в собственном или системном журнале. В зависимости от настроек, антивирус может также направлять сообщение об обнаруженном вирусе администратору сети.

Если это возможно, антивирус вылечивает файл, восстанавливая его содержимое. В противном случае предлагается только одна возможность — удалить зараженный файл и затем восстановить его из резервной копии.

Антивирусные мониторы.

Монитор автоматически проверяет все запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Интернет или скопированные на жесткий диск с дискеты и компакт диска. Антивирусный монитор сообщит пользователю, если какая-либо программа попытается выполнить потенциально опасное действие.

Обнаружение изменений.

Когда вирус заражает компьютер, он изменяет содержимое жесткого диска, например, дописывает свой код в файл программы или документа, добавляет вызов программы-вируса в файл AUTOEXEC.BAT, изменяет загрузочный сектор, создает файл-спутник. Таких изменений, однако, не делают «бестелесные» вирусы, обитающие не на диске, а в памяти процессов ОС.

Антивирусные программы, называемые ревизорами диска, не выполняют поиск вирусов по сигнатурам. Они запоминают предварительно характеристики всех областей диска, которые подвергаются нападению вируса, а затем периодически проверяют их (отсюда происходит название программы-ревизоры).

Политика безопасности

При оценке степени защищенности операционных систем действует нормативный подход, в соответствии с которым совокупность задач, решаемых системой безопасности, должна удовлетворять определенным требованиям - их перечень определяется общепринятыми стандартами. Политика безопасности

подразумевает ответы на следующие вопросы: какую информацию защищать, какого рода атаки на безопасность системы могут быть предприняты, какие средства использовать для защиты каждого вида информации.

Требования, предъявляемые к системе защиты, таковы

1. Каждый пользователь должен быть идентифицирован уникальным входным именем и паролем для входа в систему. Доступ к компьютеру предоставляется лишь после аутентификации.
2. Система должна быть в состоянии использовать уникальные идентификаторы пользователей, чтобы следить за их действиями.
3. Управление доверительными отношениями. Необходима поддержка наборов ролей (различных типов учетных записей). Кроме того, в системе должны быть средства для управления привилегированным доступом.
4. ОС должна защищать объекты от повторного использования. Перед выделением новому пользователю все объекты, включая память и файлы, должны быть проинициализированы.
5. Системный администратор должен иметь возможность учета всех событий, относящихся к безопасности (аудит безопасности).
6. Система должна защищать себя от внешнего влияния или навязывания, такого, как модификация загруженной системы или системных файлов, хранимых на диске.

Ролевой доступ. Привилегии

Понятие привилегии

С целью гибкого управления системной безопасностью в ОС Windows реализовано управление доверительными отношениями (trusted facility management), которое требует поддержки набора ролей (различных типов учетных записей) для разных уровней работы в системе

В соответствии со своей ролью каждый пользователь обладает определенными *привилегиями* и правами на выполнение различных операций в отношении системы в целом, например, право на изменение системного времени

или право на создание страничного файла. Аналогичные права в отношении конкретных объектов называются *разрешениями*. И права, и привилегии назначаются администраторами отдельным пользователям или группам как часть настроек безопасности.

Каждая привилегия имеет два текстовых представления: дружественное имя, отображаемое в пользовательском интерфейсе Windows, и программное имя, используемое приложениями, а также Luid - внутренний номер привилегии в конкретной системе.

10. Защита приложений и баз данных. Структура «пользователь(группа) – право».

Под "защитой БД" здесь понимается способ предотвратить несанкционированный доступ к информации, хранимой в таблицах.

Стандартные способы защиты

Защита с использованием пароля БД

Данный способ защиты позволяет установить пароль на открытие БД, для всех пользователей. Для его создания необходимо открыть файл БД в "монопольном" режиме и выбрать пункт меню Сервис / Защита / Задать пароль базы данных.

Защита с использованием пароля пользователя

Данный способ позволяет ввести дополнительный уровень ограничений, связанных с работой БД Access. Основан на создании файла рабочих групп, в котором определяются имена пользователей, их пароли и права на работу с различными объектами БД.

Нестандартные способы защиты

1 Изменение расширения файла

2 Защита с использованием пароля БД, содержащего непечатные символы

3 Защита с модификацией файла (Способ защиты основан на модификации первых байт файла. Таким образом, перед открытием БД в её файл записывается правильный заголовок, хранимый в программе, а после закрытия возвращается

неправильный. При попытке открыть файл БД с помощью ms Access появляется сообщение об ошибке).

4 Защита изменением версии БД

5 Защита с использованием электронного ключа

6 Шифрование значений таблиц.

11. Ролевая модель организации прав доступа к БД и приложениям.

Существует несколько способов ограничения доступа к данным:
1. дача прав в разрезе **пользователей**
2. дача прав в разрезе **ролей** + назначение ролей пользователям
3. дача прав в разрезе **групп пользователей** + определение пользователя в группу

12. Организация доступа в СУБД «клиент-сервер».(тетрадь лекция №4)

13. Подсистема информационной безопасности. Основные задачи создания п/с информационной безопасности. Типовая структура.

Наличие учетных данных пользователей и способов подключения к ресурсам, выдвигает определенные требования к корпоративной политике и правилам доступа к ресурсам:

- единый центр идентификации, авторизации и управления учетными данными пользователей;
- единая политика информационной безопасности;
- комплексная защита всех областей информационно-вычислительной системы предприятия;
- системы управления безопасностью и высокий уровень технической поддержки.

Основные задачи создания п/с информационной безопасности:

1. растущую потребность обеспечения конфиденциальности данных;

2. обеспечением непрерывности функционирования информационных систем.

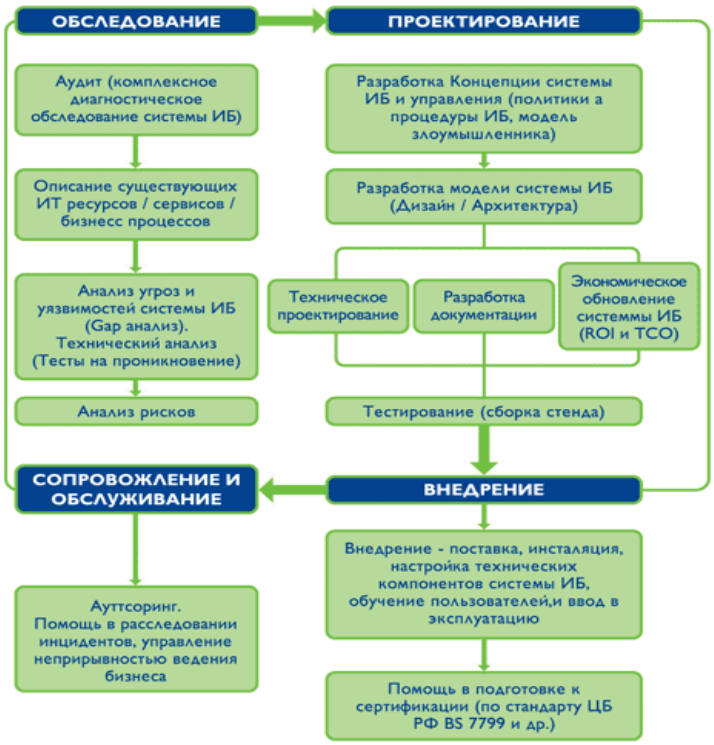


Рис. 1. Полный цикл работ по обеспечению информационной безопасности

Таким образом, при построении (модернизации) системы ИБ целесообразно реализовывать цикл работ (рис. 1), включающий обязательный этап диагностического обследования с оценкой уязвимостей информационной системы и угроз, на основе которого производится проектирование системы и ее внедрение.

14. Защита локальной рабочей станции.

1. Идентификация и аутентификация пользователей
2. Защита от загрузки с внешних носителей
3. Полномочное управление доступом
4. Разграничение доступа к устройствам
5. Замкнутая программная среда
6. Контроль целостности
7. Шифрование файлов.

15. Операторы языка SQL для обеспечения безопасности данных в СУБД.(и тетрадь)

Выдавать и забирать права доступа к таблице может владелец таблицы, Администратор Базы Данных (имеющий DBA права), а так же пользователь, которому было выдано право выдавать права (Оператором GRANT WITH GRANT OPTIONS)

```
REVOKE ALL ON customer FROM PUBLIC
GRANT ALL ON customer TO iwanow, petrow WITH GRANT OPTION
GRANT UPDATE(fname,lname,company, sity),SELECT
  ON customer TO PUBLIC
REVOKE CONNECT  FROM sidorowa, root
REVOKE DBA FROM ivanov
```

Отобрать у вас права DBA (если вы, конечно, им являетесь) может только другой DBA

```
BEGIN WORK
LOCK TABLE kadry

    . . .

UNLOCK TABLE kadry

    . . .

LOCK TABLE kadry EXCLUSIVE
```

16. Системы засекреченной связи. Общая структура, принцип функционирования.

Работу системы засекреченной связи можно описать следующим образом:
- из ключевого пространства выбирается ключ зашифрования К и отправляется по надежному каналу передачи.
- к открытому сообщению С, предназначенному для передачи, применяют преобразование F_k, определяемое ключом К, для получения зашифрованного сообщения М:$M=F_k(C)$.
- полученное зашифрованное сообщение М пересылают по каналу передачи данных.
- на принимающей стороне к полученному сообщению М применяют конкретное преобразование D_k, определяемое из всех возможных преобразований ключом К, для получения открытого сообщения С:$C=D_k(M)$.

Канал передачи данных, используемый для отправки зашифрованных сообщений, считается ненадежным, то есть любое зашифрованное сообщение может быть перехвачено противником.

17. Криптографические методы защиты информации. Понятия криптология, криптография, криптоанализ.

Криптографические методы защиты информации - это специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования. Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а не доступ к ней (например, зашифрованный файл нельзя прочесть даже в случае кражи носителя). Данный метод защиты реализуется в виде программ или пакетов программ.

Современная криптография включает в себя четыре крупных раздела:

1. *Симметричные криптосистемы*. В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ;

2. *Криптосистемы с открытым ключом*. В системах с открытым ключом используются два ключа - открытый и закрытый, которые математически связаны друг с другом;

3. *Электронная подпись*. Системой электронной подписи называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

4. *Управление ключами*. Это процесс системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Криптология — наука, занимающаяся методами шифрования и дешифрования. Криптология состоит из двух частей — криптография и криптоанализ.

Криптография — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст).

Криптоанализ — наука о методах получения исходного значения зашифрованной информации, не имея доступа к секретной информации (ключу), необходимой для этого. В большинстве случаев под этим подразумевается нахождение ключа. Под термином «криптоанализ» также понимается попытка найти уязвимость в криптографическом алгоритме или протоколе.

18. Стойкость алгоритма шифрования. Теория Шеннона.

Используя теорию вероятности и математическую статистику, Шеннон решил оптимальный способ передачи информации: при рассмотрении стойкости криптографических систем, Шеннон ввел понятие:

- теоретической стойкости
- практической стойкости

Теоретическая стойкость: насколько надежна система, если криптоаналитик противника не ограничен временем и обладает всеми необходимыми вычислительными средствами для анализа.

Практическая стойкость: надежна ли система, если криптоаналитик располагает ограниченным временем и ограниченными вычислительными возможностями для анализа перехваченных криптограмм.

По теории Шеннона, чтобы алгоритм считался абсолютно стойким, он должен удовлетворять следующим требованиям:

1. длина ключа и длина открытого текста должны быть одинаковы
2. ключ должен использоваться только один раз.

На практике для увеличения стойкости систем криптозащиты Шеннон выделил 2 общих принципа:

1. рассеивание
2. перемешивание

Рассеивание: распространение влияния одного знака, открытого текста на много знаков криптограммы с тем, чтобы скрыть статистические свойства открытого текста.

Перемешивание: использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических средств открытого текста и криптограммы.

Для достижения свойств рассеивания и перемешивания широко используются составные шифры, состоящие из последовательности простых шифров.

19. Классификация алгоритмов шифрования.

- Симметричные (с секретным, единым ключом, одноключевые, single-key).

- Потоковые (шифрование потока данных):
  - с одноразовым или бесконечным ключом (infinite-key cipher);
  - с конечным ключом (система Вернама);
  - на основе генератора псевдослучайных чисел (ПСЧ).
- Блочные (шифрование данных поблочно):
  - Шифры перестановки (permutation, P-блоки);
  - Шифры замены (подстановки, substitution, S-блоки):
  - моноалфавитные (код Цезаря);
  - полиалфавитные (шифр Вижинера, цилиндр Джефферсона, диск Уэтстоуна, Enigma);
- Составные:
  - Lucipher (фирма IBM, США);
  - DES (Data Encryption Standard, США);
  - FEAL-1 (Fast Enciphering Algoritm, Япония);
  - IDEA/IPES (International Data Encryption Algorithm/
  - Improved Proposed Encryption Standard, фирма Ascom-Tech AG, Швейцария);
  - B-Crypt (фирма British Telecom, Великобритания);
  - ГОСТ 28147-89 (СССР); * Skipjack (США).

• Асимметричные (с открытым ключом, public-key):

- Диффи-Хеллман DH (Diffie, Hellman);
- Райвест-Шамир-Адлеман RSA (Rivest, Shamir, Adleman);
- Эль-Гамаль ElGamal.

20. Шифры замены и перестановки (привести примеры).

Шифром замены называется алгоритм шифрования, который производит замену каждой буквы открытого текста на какой-то символ шифрованного текста. Получатель сообщения расшифровывает его путем обратной замены.

В классической криптографии различают 4 разновидности шифров замены:

▪ *Простая замена,* или *одноалфавитный шифр.* Каждая буква открытого текста заменяется на один и тот же символ шифртекста.

▪ *Омофонная замена.* Аналогична простой замене с единственным отличием: каждой букве открытого текста ставятся в соответствие несколько символов шифртекста. Например, буква "А" заменяется на цифру 5, 13, 25 или 57 , а буква "Б" — на 7, 19, 31 или 43 и так далее.

▪ *Блочная замена.* Шифрование открытого текста производится блоками. Например, блоку "АБА" может соответствовать "РТК", а блоку "АББ" — "СЛЛ".

▪ *Многоалфавитная замена*. Состоит из нескольких шифров простои замены. Например, могут использоваться пять шифров простой замены, а какой из них конкретно применяется для шифрования данной буквы открытого текста, — зависит от ее положения в тексте.

Шифры перестановки.

В *шифре перестановки* буквы открытого текста не замещаются на другие, а меняется сам порядок их следования. Например, в шифре простой колонной перестановки исходный открытый текст записывается построчно (число букв в строке фиксировано), а шифртекст получается считыванием букв по колонкам. Расшифрование производится аналогично: шифртекст записывается поколонно, а открытый текст можно затем прочесть по горизонтали.

Для повышения стойкости полученный шифртекст можно подать на вход второго шифра перестановки. Существуют еще более сложные шифры перестановки, однако почти все они легко взламываются с помощью компьютера.

Хотя во многих современных криптографических алгоритмах и используется перестановка, ее применение ограничено узкими рамками, поскольку в этом случае требуется память большого объема, а также накладываются ограничения на длину шифруемых сообщений. Замена получила значительно большее распространение.

21. Шифрование методом гаммирования.

Под гаммированием понимают процесс наложения по определенному закону гаммы шифра на открытые данные. Гамма шифра - это псевдослучайная

последовательность, выработанная по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных.

Процесс зашифрования заключается в генерации гаммы шифра и наложении полученной гаммы на исходный открытый текст обратимым образом, например с использованием операции сложения по модулю 2.

Следует отметить, что перед зашифрованием открытые данные разбивают на блоки T_0^i одинаковой длины, обычно по 64 бита. Гамма шифра вырабатывается в виде последовательности блоков $Г_ш^i$ аналогичной длины.

Уравнение зашифрования можно записать в виде:

$$T_ш^i = Г_ш^i \oplus T_0^i, \quad i = 1...M, \tag{1}$$

где $T_ш^i$ - i-й блок шифртекста; $Г_ш^i$ - i-й блок гаммы шифра; T_0^i -i-й блок открытого текста; M - количество блоков открытого текста. $T_ш$

Процесс расшифрования сводится к повторной генерации гаммы шифра и наложению этой гаммы на зашифрованные данные. Уравнение расшифрования имеет вид:

$$T_0^i = Г_ш^i \oplus T_ш^i, \tag{17}$$

Получаемый этим методом шифртекст достаточно труден для раскрытия, поскольку теперь ключ является переменным. По сути дела гамма шифра должна изменяться случайным образом для каждого шифруемого блока. Если период гаммы превышает длину всего шифруемого текста и злоумышленнику неизвестна никакая часть исходного текста, то такой шифр можно раскрыть только прямым перебором всех вариантов ключа. В этом случае криптостойкость шифра определяется длиной ключа.

22. Шифрование и дешифрование по методу Вижинера.

Для расшифрования и зашифрования информации используется таблица Вижинера.

Таблица Вижинера представляет собой квадратную матрицу с n^2 элементами, где n -число символов используемого алфавита. Каждая строка получается циклическим сдвигом алфавита на один символ влево.

Для шифрования выбирается буквенный ключ, в соответствии с которым формируется рабочая матрица: из полной матрицы выбираются строки, начинающиеся с символов ключа.

Процесс шифрования следующий: под каждой буквой исходного текста подписываются буквы ключа, и при необходимости (если ключ оказался короче сообщения) ключ циклически повторяется нужное количество раз. Каждая буква шифруемого текста заменяется по рабочей матрице буквами, находящимися на пересечении линий, соединяющих буквы исходного текста и строк, находящихся под ними букв ключа.

Расшифрование текста осуществляется в обратном порядке: над буквами зашифрованного текста последовательно подписываются буквы ключа. Поскольку процесс обратный, в строке букв ключа отыскиваются нужные буквы криптограммы, и буквой открытого текста будет буква, стоящая в первой строке над этой буквой криптограммы.

Недостатки: при небольшой длине ключа надежность шифрования невысока, а формирование длинного ключа сопряжено с определенными трудностями.

23. Требования к криптографическому закрытию информации.

1. Сложность и стойкость криптографического закрытия данных должны выбираться в зависимости от объема и степени секретности данных.

2. Надежность закрытия должна быть такой, чтобы секретность не нарушалась даже в том случае, когда злоумышленнику становится известен метод шифрования.

3. Метод закрытия, набор используемых ключей и механизм их распределения не должны быть слишком сложными.

4. Выполнение процедур прямого и обратного преобразований должно быть формальным. Эти процедуры не должны зависеть от длины сообщений.

5. Ошибки, возникающие в процессе преобразования не должны распространяться по системе.

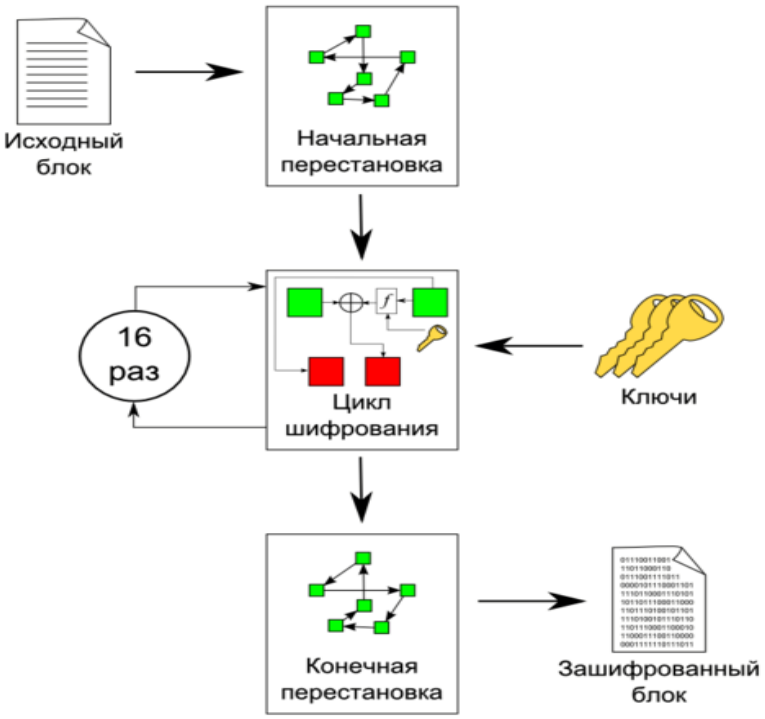
6. Вносимая процедурами защиты избыточность должна быть минимальной.

24. Стандарт на шифрование. Общее описание DES-алгоритма.

DES (*Data Encryption Standard*) — симметричный алгоритм шифрования, в котором один ключ используется как для шифрования, так и для расшифрования данных. DES разработан фирмой IBM и утвержден правительством США в 1977 году как официальный стандарт (FIPS 46-3). DES имеет блоки по 64 бит и 16 цикловую структуру сети Фейстеля, для шифрования использует ключ с длиной 56 бит. Алгоритм использует комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований. Для DES рекомендовано несколько режимов:

- режим электронной кодовой книги (ECB — Electronic Code Book) ,
- режим сцепления блоков (CBC — Cipher Block Chaining),
- режим обратной связи по шифротексту (CFB — Cipher Feed Back),
- режим обратной связи по выходу (OFB — Output Feed Back).

Блок – схема DES:



Входные 64 – битовые блоки открытого текста преобразуются в выходные 64 – битовые векторы с помощью двоичного 56 – битового ключа . Число различных ключей алгоритма равно 2^{256}. Алгоритм реализуется в течении 16 аналогичных циклов шифрования, где на i – м цикле используется свой цикловой ключ K_i , представляющий собой алгоритмически вырабатываемую выборку 48 битов из 56 битового ключа.

Сначала 64 бита входной последовательности перестанавливаются в соответствии с заданной таблицей перестановок. Полученная последовательность бит разделяется на 2 полу последовательности L(0) – левые(старшие) биты и R(0)- младшие (правые) биты, каждый из которых содержит соответственно 32 бита. Затем выполняется процесс шифрования, который описывается следующими формулами:

L(i) = R(i-1)

R(i) = L(i-1)+f(R(i-1) , K(i)), i = 1..16

Функция f называется функцией процесс шифрования. Ее аргументами являются :

- последовательность R, полученная на предыдущем шаге итерации

•48 – битовый ключ.

Требуемые 16 48-битовых ключей генерируется из исходных 56-битового ключа по определенному алгоритму шифрования.

На последующем шаге итерации будут получены R(16) и L(16), которые сцепляются в 64 – битовую последовательность, которая перестанавливается в соответствии с таблицей конечной перестановки. Выходная последовательность готова.

25. Ключевая система алгоритмов шифрования.

26. Криптографические протоколы.

Стандартным подходом к обеспечению безопасности для групп является получение некоторой секретной величины, известной только участникам группы. Криптографические протоколы, в которых происходят выработка и распространение этой величины внутри группы известны как *распределение ключа группы (group key establishment)*. В случае, когда это значение не вырабатывается в протоколе, а приобретается заранее кем-либо из участников, протокол носит название *протокола распространения ключей в группе(group key distribution).*

Протокол обмена для выработки общего ключа (key agreement protocol) – протокол распределения ключей, в котором общий ключ вырабатывается двумя или более участниками как функция от информации, вносимой каждым из них, причем таким образом, что никакая другая сторона не может предопределить получаемый в результате общий секрет.

Протоколы обмена должны обладать следующими свойствами:

- совершенная опережающая секретность (*Perfect forward secrecy – PFS*);
- устойчивость к атакам по известному ключу (*Known-key attacks*);
- аутентификации ключа (*Key authentication*);
- подтверждение и целостность ключа (*Key confirmation & key integrity*).

Протокол обеспечивает *PFS*, если компрометация долговременных ключей не компрометирует сеансовых ключей.

Протокол обладает свойством *контрибутивности (contributory)*, если сформированный ключ зависит от секретных данных, внесенных каждым из участников.

Пусть R – протокол обмена для n участников, M – множество участников, а S_n – ключ, получаемый в результате протокола R. Тогда R обеспечивает *неявную аутентификацию ключа (implicit key authentication)*, если каждый $M_i \square M$ уверен, что никакая другая сторона $M_q \square M$ не могла получить доступ к S_n (за исключением злоумышленника M_j внутри группы).

Протокол обеспечивает *подтверждение ключа*, если участник протокола уверен, что другой участник (или группа) действительно обладает ключом, полученным в результате протокола.

Контрибутивный протокол обмена обеспечивает *целостность ключа*, если участник уверен, что полученный им секретный ключ представляет собой функцию ТОЛЬКО от индивидуальных вкладов всех других участников. Таким образом, любое вмешательство в сформированный ключ (или формируемый) нарушает данное свойство, если ключ получается отличным от предполагаемого.

27. Концепция криптосистем с открытым ключом.

Эффективными системами криптографической защиты данных являются асимметричные криптосистемы, называемые также криптосистемами с открытым ключом. В таких системах для зашифрования данных используется один ключ, а для расшифрования - другой ключ (отсюда и название - асимметричные). Первый ключ является открытым и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифрование данных с помощью открытого ключа невозможно.

Для расшифрования данных получатель зашифрованной информации использует второй ключ, который является секретным. Разумеется, ключ расшифрования не может быть определен из ключа зашифрования.

В этой криптосистеме применяют два различных ключа: $К_В$ - открытый ключ получателя В, которым будет шифровать отправитель А; $k_В$ - секретный ключ получателя В. Генератор ключей целесообразно располагать на стороне

получателя B (чтобы не пересылать секретный ключ $К_B$ по незащищенному каналу). Значения ключей $К_B$ и k_B зависят от начального состояния генератора ключей.

Раскрытие секретного ключа k_B по известному открытому ключу $К_B$ должно быть вычислительно неразрешимой задачей.

Характерные особенности асимметричных криптосистем:

1. Открытый ключ $К_B$ и криптограмма C могут быть отправлены по незащищенным каналам, т.е. противнику известны $К_B$ и C.

2. Алгоритмы шифрования и расшифрования

E_B: M → C,

D_B: C → M,

являются открытыми.

28. Электронная цифровая подпись. Структурная схема построения ЭЦП.

Электронная цифровая подпись (**ЭЦП**) — реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭЦП и проверить принадлежность подписи владельцу сертификата ключа ЭЦП. Значение реквизита получается в результате криптографического преобразования информации с использованием *закрытого ключа ЭЦП.*

Существует несколько схем построения цифровой подписи:

- На основе алгоритмов симметричного шифрования. Данная схема предусматривает наличие в системе третьего лица — арбитра, пользующегося доверием обеих сторон. Авторизацией документа является сам факт зашифрования его секретным ключом и передача его арбитру.
- На основе алгоритмов асимметричного шифрования. На данный момент такие схемы ЭЦП наиболее распространены и находят широкое применение.

Кроме этого, существуют другие разновидности цифровых подписей (групповая подпись, неоспоримая подпись, доверенная подпись), которые

являются модификациями описанных выше схем. Их появление обусловлено разнообразием задач, решаемых с помощью ЭЦП.

Общепризнанная схема цифровой подписи охватывает три процесса:

- **Генерация** ключевой пары. При помощи алгоритма генерации ключа равновероятным образом из набора возможных закрытых ключей выбирается закрытый ключ, вычисляется соответствующий ему открытый ключ.
- **Формирование подписи**. Для заданного электронного документа с помощью закрытого ключа вычисляется подпись.
- **Проверка (верификация) подписи**. Для данных документа и подписи с помощью открытого ключа определяется действительность подписи.

Для того, чтобы использование цифровой подписи имело смысл, необходимо выполнение двух условий:

- Верификация подписи должна производиться открытым ключом, соответствующим именно тому закрытому ключу, который использовался при подписании.
- Без обладания закрытым ключом должно быть вычислительно сложно создать легитимную цифровую подпись.

29. Стеганография. Определение. Обобщённая модель стегосистемы.

Стеганография — это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает само его существование. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

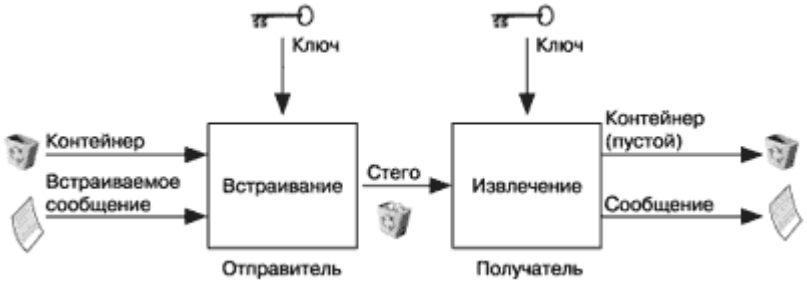
Стеганография - это метод организации связи, который собственно скрывает само наличие связи. В отличие от криптографии, где неприятель точно может определить является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в безобидные

послания так, чтобы невозможно было заподозрить существование встроенного тайного послания.

При построении стегосистемы должны учитываться следующие положения:

- противник имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, которая остается неизвестной потенциальному противнику, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;
- если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения в других данных до тех пор, пока ключ хранится в тайне;
- потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

Обобщенная модель стегосистемы представлена на рис. 2.



В качестве данных может использоваться любая информация: текст, сообщение, изображение и т. п.

В общем же случае целесообразно использовать слово "сообщение", так как сообщением может быть как текст или изображение, так и, например, аудиоданные. Далее для обозначения скрываемой информации, будем использовать именно термин сообщение.

Контейнер - любая информация, предназначенная для сокрытия тайных сообщений.

Пустой контейнер - контейнер без встроенного сообщения; заполненный контейнер или стего - контейнер, содержащий встроенную информацию.

Встроенное (скрытое) сообщение - сообщение, встраиваемое в контейнер.

Стеганографический канал или просто стегоканал - канал передачи стего.

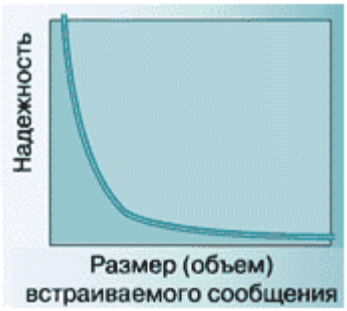
Стегоключ или просто ключ - секретный ключ, необходимый для сокрытия информации. В зависимости от количества уровней защиты (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей.

30. Требования к стегосистемам. Надёжность стегосистем.

Любая стегосистема должна отвечать следующим требованиям:

- Свойства контейнера должны быть модифицированы, чтобы изменение невозможно было выявить при визуальном контроле. Это требование определяет качество сокрытия внедряемого сообщения: для обеспечения беспрепятственного прохождения стегосообщения по каналу связи оно никоим образом не должно привлечь внимание атакующего.
- Стегосообщение должно быть устойчиво к искажениям, в том числе и злонамеренным. В процессе передачи изображение (звук или другой контейнер) может претерпевать различные трансформации: уменьшаться или увеличиваться, преобразовываться в другой формат и т. д. Кроме того, оно может быть сжато, в том числе и с использованием алгоритмов сжатия с потерей данных.
- Для сохранения целостности встраиваемого сообщения необходимо использование кода с исправлением ошибки.
- Для повышения надежности встраиваемое сообщение должно быть продублировано.

Для большинства современных методов, используемых для сокрытия сообщения в цифровых контейнерах, имеет место следующая зависимость надежности системы от объема встраиваемых данных (рис. 3).



Данная зависимость показывает, что при увеличении объема встраиваемых данных снижается надежность системы (при неизменности размера контейнера). Таким образом, используемый в стегосистеме контейнер накладывает ограничения на размер встраиваемых данных.

31. Защита информации в сетях Internet. Назначение экранирующих систем.

Экран – это средство разграничения доступа клиентов из одного множества к серверам из другого множества. Экран выполняет свои функции, контролируя все информационные потоки между двумя множествами систем.

В простейшем случае экран состоит из двух механизмов, один из которых ограничивает перемещение данных, а второй, наоборот, ему способствует. В более общем случае экран или полупроницаемую оболочку удобно представлять себе как последовательность фильтров. Каждый из них может задержать данные, а может и сразу "перебросить" их "на другую сторону". Кроме того, допускаются передача порции данных на следующий фильтр для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю.

При работе в Интернете следует иметь в виду, что насколько ресурсы Всемирной сети открыты каждому клиенту, настолько же и ресурсы его компьютерной системы могут быть при определенных условиях открыты всем, кто обладает необходимыми средствами. Для частного пользования этот факт не играет особой роли, но знать о нем необходимо, чтобы не допускать действий, нарушающих законодательства тех стран, на территории которых расположены серверы Интернета. К таким действиям относятся вольные или невольные попытки нарушить работоспособность компьютерных систем, попытки взлома

защищенных систем, использование и распространение программ, нарушающих работоспособность компьютерных систем (в частности, компьютерных вирусов). Работая во Всемирной сети, следует помнить о том, что абсолютно все действия фиксируются и протоколируются специальными программными средствами и информация как о законных, так и о незаконных действиях обязательно где-то накапливается. Таким образом, к обмену информацией в Интернете следует подходить как к обычной переписке с использованием почтовых открыток. Информация свободно циркулирует в обе стороны, но в общем случае она доступна всем участникам информационного процесса. Это касается всех служб Интернета, открытых для массового использования. Однако даже в обычной почтовой связи наряду с открытками существуют и почтовые конверты. Использование почтовых конвертов при переписке не означает, что партнерам есть, что скрывать. Их применение соответствует давно сложившейся исторической традиции и устоявшимся морально-этическим нормам общения. Потребность в аналогичных "конвертах" для защиты информации существует и в Интернете. Сегодня Интернет является не только средством общения и универсальной справочной системой - в нем циркулируют договорные и финансовые обязательства, необходимость защиты которых как от просмотра, так и от фальсификации очевидна.

Принцип защиты информации в Интернете основан на том, чтобы исключить или, по крайней мере, затруднить возможность подбора *адекватного* метода для преобразования данных в информацию. Одним из приемов такой защиты является *шифрование* данных.

НАЗНАЧЕНИЕ ЭКРАНИРУЮЩИХ СИСТЕМ.

Проблема межсетевого экранирования формулируется следующим образом. Пусть имеется две информационные системы или два множества информационных систем. Экран (firewall) - это средство разграничения доступа клиентов из одного множества систем к информации, хранящейся на серверах в другом множестве.

Экран выполняет свои функции, контролируя все информационные потоки между

этими двумя множествами информационных систем, работая как некоторая “информационная мембрана”. В этом смысле экран можно представлять себе как набор фильтров, анализирующих проходящую через них информацию и, на основе заложенных в них алгоритмов, принимающих решение: пропустить ли эту информацию или отказать в ее пересылке. Кроме того, такая система может выполнять регистрацию событий, связанных с процессами разграничения доступа. в частности, фиксировать все “незаконные” попытки доступа к информации и, дополнительно, сигнализировать о ситуациях, требующих немедленной реакции, то есть поднимать тревогу.
Обычно экранирующие системы делают несимметричными. Для экранов определяются понятия “внутри” и “снаружи”, и задача экрана состоит в защите внутренней сети от “потенциально враждебного” окружения. Важнейшим примером потенциально враждебной внешней сети является Internet.
Рассмотрим более подробно, какие проблемы возникают при построении экранирующих систем. При этом мы будем рассматривать не только проблему безопасного подключения к Internet, но и разграничение доступа внутри корпоративной сети организации.

32. Требования к построению экранирующих систем.

1. обеспечение безопасности внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи;
2. экранирующая система должна обладать мощными и гибкими средствами управления для простого и полного воплощения в жизнь политики безопасности организации и, кроме того, для обеспечения простой реконфигурации системы при изменении структуры сети;
3. экранирующая система должна работать незаметно для пользователей локальной сети и не затруднять выполнение ими легальных действий;
4. экранирующая система должна работать достаточно эффективно и успевать обрабатывать весь входящий и исходящий трафик в “пиковых” режимах;
5. Система обеспечения безопасности должна быть сама надежно защищена от любых несанкционированных воздействий, поскольку она является ключом к

конфиденциальной информации в организации;
6. В идеале, если у организации имеется несколько внешних подключений, в том числе и в удаленных филиалах, система управления экранами должна иметь возможность централизованно обеспечивать для них проведение единой политики безопасности;
7. Система должна иметь средства авторизации доступа пользователей через внешние подключения. Типичной является ситуация, когда часть персонала организации должна выезжать, например, в командировки, и в процессе работы им, тем немение, требуется доступ, по крайней мере, к некоторым ресурсам внутренней компьютерной сети организации. Система должна уметь надежно распознавать таких пользователей и предоставлять им необходимый доступ к информации.

33. Организация политики безопасности в сетях Internet с помощью пакета Solstice FireWall-1.

Классическим примером, является программный комплекс Solstice FireWall-1 компании Sun Microsystems. Данный пакет неоднократно отмечался наградами на выставках и конкурсах. Он обладает многими полезными особенностями, выделяющими его среди продуктов аналогичного назначения. Рассмотрим основные компоненты Solstice FireWall-1 и функции, которые они реализуют.

Центральным для системы FireWall-1 является модуль управления всем комплексом. С этим модулем работает администратор безопасности сети. Следует отметить, что продуманность и удобство графического интерфейса модуля управления отмечалось во многих независимых обзорах, посвященных продуктам данного класса.

Основные компоненты Solstice FireWall-1 .

Администратору безопасности сети для конфигурирования комплекса FireWall-1 необходимо выполнить следующий ряд действий:

• Определить объекты, участвующие в процессе обработки информации. Здесь

имеются в виду пользователи и группы пользователей, компьютеры и их группы, маршрутизаторы и различные подсети локальной сети организации.
• Описать сетевые протоколы и сервисы, с которыми будут работать приложения. Впрочем, обычно достаточным оказывается набор из более чем 40 описаний, поставляемых с системой FireWall-1.
• Далее, с помощью введенных понятий описывается политика разграничения доступа в следующих терминах: “Группе пользователей А разрешен доступ к ресурсу Б с помощью сервиса или протокола С, но об этом необходимо сделать пометку в регистрационном журнале”. Совокупность таких записей компилируется в исполнимую форму блоком управления и далее передается на исполнение в модули фильтрации.
Модули фильтрации могут располагаться на компьютерах - шлюзах или выделенных серверах - или в маршрутизаторах как часть конфигурационной информации. В настоящее время поддерживаются следующие два типа маршрутизаторов: Cisco IOS 9.x, 10.x, а также BayNetworks (Wellfleet) OS v.8. Модули фильтрации просматривают все пакеты, поступающие на сетевые интерфейсы, и, в зависимости от заданных правил, пропускают или отбрасывают эти пакеты, с соответствующей записью в регистрационном журнале. Следует отметить, что эти модули, работая непосредственно с драйверами сетевых интерфейсов, обрабатывают весь поток данных, располагая полной информацией о передаваемых пакетах.

34. Защита информационных систем на логическом, физическом и юридическом уровнях.

Методы защиты информации в автоматизированных системах обработки данных

1. Ограничение доступа
2. Разграничение доступа
3. Разделение доступа (привилегий)
4. Криптографическое преобразование информации

5. Контроль и учет доступа

6. Законодательные меры

Ограничение доступа. Заключается в создании некоторой замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с этим объектом, защиты по своим функциональным обязанностям. Ограничение доступа заключается в следующем:

- выделение специальной территории для размещения объекта
- сооружение по периметру зоны специального ограждения с охранной сигнализацией
- создание контрольно-пропускного режима на территории зданий и помещений

Задача средств ограничения доступа: исключить случайный и преднамеренный доступ посторонних лиц на защищаемую территории. С этой целью создаются замкнутый контур с 2-мя видами преград физическим и контрольно-пропускной функцией, охранная сигнализация.

Разграничение и контроль доступа к информации. Разграничение доступа в вычислительной системе заключается в разделении информации на потоки и организации к ней доступа в соответствии с функциональными обязанностями и полномочиями.

Задача: сократить количество лиц допускаемых к информации, т.е. защита информации от нарушителей среди допущенного к ней персонала. При этом деление может производится:

- по степени важности
- по секретности
- по функциональному назначению

Прежде всего нужно разграничить доступ к специальным средсвам. Тех обслуживание должны производится спец персоналом без доступа к информации. Перезагрузка и настройка должна производиться специально выделенным специалистом. Функции безопасности информации должны обеспечиваться владельцем этой информации. Организация доступа пользователей должна

обеспечить разграничение доступа. Разграничение доступа пользователей могут осуществляться по следующим параметрам:

- по виду
- характеру
- назначению и степени важности

По способам обработки

- читать
- писать
- изменять
- удалять

По условному номеру терминала.

Причины определяющие важность проблемы защиты информации:

1. Высокие темпы роста парка ПЭВМ ;
2. Широкое применение ПЭВМ в различных сферах деятельности;
3. Высокая степень концентрации информации в ПЭВМ;
4. Совершенствование способов доступа пользователей к ресурсам ПЭВМ;
5. Усложнение вычислительного процесса ПЭВМ.

Объектами посягательств могут быть сами технические средства (компьютерная периферия) как материальные объекты так и ПО, БД, для которых технические средства являются окружением.

Если ПК только объект посягательства, то определение права нарушения может быть произведено по существующим нормам права. Если хищение информации связано с потерей материальных и финансовых ценностей, то этот факт можно квалифицировать как преступление. Так же, если с данным фактом связывается нарушение интересов национальной безопасности, авторского права, то уголовная ответственность прямо предусматривается в рамках закона УК. Основным законом регламентирующим отношения в области ИТ и ИС, закон не затрагивает отношений регулируемых законом РФ «Об авторском праве и

смежных правах» является ФЗ 20.02.95 «Об информации, информатизации, защите информации».

Цели защиты информации:

1. Предотвращение утечки, хищений, утраты, искажения, подделки информации;
2. Предотвращение угроз безопасности жизни, общества, государства;
3. Защита конституционных прав граждан на сохранение личных тайн;
4. Сохранение государственных тайн;
5. Обеспечение прав субъектов в информационных процессах;

Компьютерные преступления можно подразделить на 2-е категории:

1. Преступления связанные с вмешательством в работу компьютера;
2. Преступления использующие компьютеры как технические средства.

Виды преступлений:

1. Несанкционированный доступ к информации;
2. Ввод в ПО «логических бомб», которые срабатывают при выполнении определенных условий;
3. Разработка и распространение компьютерных вирусов;
4. Небрежность в разработке изготовления и эксплуатация программных и вычислительных комплексов, приводящих к тяжким последствиям;

34. Российское законодательство в области защиты информации.

В Российской Федерации к нормативно-правовым актам в области информационной безопасности относятся:

- Акты федерального законодательства:
  - Международные договоры РФ;
  - Конституция РФ;
  - Законы федерального уровня (включая федеральные конституционные законы, кодексы);
  - Указы Президента РФ;

- Постановления правительства РФ;
- Нормативные правовые акты федеральных министерств и ведомств;
- Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

К нормативно-методическим документам можно отнести

- Методические документы государственных органов России:
  - Доктрина информационной безопасности РФ;
  - Руководящие документы ФСТЭК (Гостехкомиссии России);
  - Приказы ФСБ;
- Стандарты информационной безопасности, из которых выделяют:
  - Международные стандарты;
  - Государственные (национальные) стандарты РФ;
  - Рекомендации по стандартизации;
  - Методические указания.

35. Программные и программно-аппаратные комплексы средств защиты информации. Их основные функции.

Программными называются средства защиты данных, функционирующие в составе программного обеспечения. Среди них можно выделить следующие:

- средства архивации данных;
- антивирусные программы;
- криптографические средства;
- средства идентификации и аутентификации пользователей;
- средства управления доступом;
- протоколирование и аудит.

Как примеры комбинаций вышеперечисленных мер можно привести:

- защиту баз данных;
- защиту информации при работе в компьютерных сетях.

Средства архивации информации

Иногда резервные копии информации приходится выполнять при общей ограниченности ресурсов размещения данных, например владельцам персональных компьютеров. В этих случаях используют программную архивацию. Архивация это слияние нескольких файлов и даже каталогов в единый файл — архив, одновременно с сокращением общего объема исходных файлов путем устранения избыточности, но без потерь информации, т. е. с возможностью точного восстановления исходных файлов Наиболее известны и популярны следующие архивные форматы:

- ZIP, ARJ для операционных систем DOS и Windows;
- TAR для операционной системы Unix;
- межплатформный формат JAR (Java ARchive);
- RAR (все время растет популярность этого нового формата, так как разработаны программы позволяющие использовать его в операционных системах DOS, Windows и Unix).

Программно-аппаратные средства защиты

Программно-аппаратные системы защиты - средства, основанные на использовании так называемых "аппаратных электронных ключей". Электронный ключ - это аппаратная часть системы защиты, представляющая собой плату с микросхемами памяти и, в некоторых случаях, микропроцессором, помещенную в корпус и предназначенную для установки в один из стандартных портов ПК (COMM, USB ...) или слот расширения материнской платы. Так же в качестве такого устройства могут использоваться смарт-карта. По результатам проведенным анализа, программно-аппаратные средства защиты в настоящий момент являются одними из самых стойких систем защиты ПО.

С точки зрения производителя ПО программно-аппаратные средства защиты обладают определенными положительными и отрицательными качествами, в том числе:

Положительные факторы: значительное затруднение нелегального распространения и использования ПО, избавление производителя ПО от необходимости разработки собственной системы защиты, высокая автоматизация

процесса защиты ПО, возможность легкого создания демо-версий, достаточно большой выбор таких систем на рынке, повышение <престижности> ПО при наличии мощной защиты.

Отрицательные факторы: затруднение разработки и отладки ПО из-за ограничений со стороны системы защиты (так же почти невозможно распространение "заплаток"), дополнительные затраты на приобретение системы защиты и обучение персонала, замедление продаж из-за необходимости физической передачи аппаратной части, повышение системных требований из-за защиты (совместимость, драйверы), снижение доверия пользователей при некорректной реализации защиты.