Лекция № 8

Компьютерная безопасность

8.1. Понятие компьютерной безопасности

В вычислительной технике понятие безопасности является весьма широким. Оно подразумевает

1. надежность работы компьютера,
2. сохранность ценных данных,
3. защиту информации от внесения в нее изменений неуполномоченными лицами,
4. сохранение тайны переписки при электронной связи.

Разумеется, во всех цивилизованных странах на страже безопасности граждан стоят законы, но в сфере вычислительной техники правоприменительная практика пока развита недостаточно, а законотворческий процесс не успевает за развитием технологий.

Надежность работы компьютерных систем опирается на меры самозащиты.

8.2. Компьютерные вирусы

Компьютерный вирус — это программный код, встроенный в другую программу, или в документ, или в определенные области носителя данных и предназначенный для выполнения несанкционированных действий на несущем компьютере.

Основными типами компьютерных вирусов являются:

- **программные вирусы;**
- **загрузочные вирусы;**
- **макровирусы.**

К компьютерным вирусам примыкают и так называемые ***троянские кони*** *(троянские программы, троянцы).*

8.2.1. Программные вирусы

Программные вирусы — это блоки программного кода, целенаправленно внедрённые внутрь других прикладных программ.

При запуске программы, несущей вирус, происходит запуск имплантированного в нее вирусного кода. Работа этого кода вызывает скрытые от пользователя изменения в файловой системе жестких дисков и/или в содержании других программ.

Так, например, вирусный код может воспроизводить себя в теле других программ — этот процесс **называется размножением**.

По прошествии определённого времени, создав достаточное количество копий, программный вирус может перейти к разрушительным действиям — нарушению работы программ и операционной системы, удалению информации, хранящейся на жестком диске.

Этот процесс называется **вирусной атакой**.

8.2.1. Программные вирусы-классификация

1. Самые разрушительные вирусы могут инициировать форматирование жестких дисков. Поскольку форматирование диска — достаточно продолжительный процесс, который не должен пройти незамеченным со стороны пользователя.

2. Во многих случаях **программные вирусы ограничиваются уничтожением данных только в системных секторах жесткого диска**, что эквивалентно потере таблиц файловой структуры.

В этом случае данные на жестком диске остаются нетронутыми, но воспользоваться ими без применения специальных средств нельзя, поскольку неизвестно, какие сектора диска каким файлам принадлежит.

Теоретически восстановить данные в этом случае можно, но трудоемкость этих работ исключительно высока.

8.2.1. Программные вирусы-классификация

3. Считается, что никакой вирус не в состоянии вывести из строя аппаратное обеспечение компьютера.

Однако бывают случаи, когда аппаратное и программное обеспечение настолько взаимосвязаны, что программные повреждения приходится устранять заменой аппаратных средств.

Так, например, в большинстве современных материнских плат базовая система ввода-вывода (BIOS) хранится в перезаписываемых постоянных запоминающих устройствах (так называемая флэш-память).

Возможность перезаписи информации в микросхеме флэш-памяти используют некоторые программные вирусы для уничтожения данных BIOS.

В этом случае для восстановления работоспособности компьютера требуется либо замена микросхемы, хранящей BIOS, либо ее перепрограммирование на специальных устройствах, называемых программаторами.

8.2.1. Программные вирусы – источники заражения

1. Программные вирусы поступают на компьютер при запуске непроверенных программ, полученных на внешнем носителе (флеш-диск, компакт-диск и т. п.) или принятых из Интернета.

2. Особое внимание следует обратить на слова при запуске. **При обычном копировании зараженных файлов заражение компьютера произойти не может.**

3. В связи с этим все данные, принятые из Интернета, должны проходить обязательную проверку на безопасность, а если получены незатребованные данные из незнакомого источника, их следует уничтожать, не рассматривая.

4. Обычный прием распространения «троянских» программ — приложение к электронному письму с «рекомендацией» извлечь и запустить якобы полезную программу.

8.2.2. Загрузочные вирусы

От программных вирусов **загрузочные вирусы** отличаются методом распространения.

Загрузочные вирусы поражают не программные файлы, а определенные системные области магнитных носителей (жестких и флеш дисков).

Кроме того, на включенном компьютере они могут временно располагаться в оперативной памяти.

Обычно заражение происходит при попытке загрузки компьютера с магнитного носителя, системная область которого содержит загрузочный вирус.

Так, например, при попытке загрузить инсталляционную компьютерную программу с внешнего носителя или из интернет происходит сначала проникновение вируса в оперативную память, а затем в загрузочный сектор жестких дисков. Далее этот компьютер сам становится источником распространения загрузочного вируса.

8.2.3. Макровирусы

Макровирусы - это особая разновидность вирусов, которая поражает документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения так называемых макрокоманд.

В частности, к таким документам относятся документы текстового процессора Microsoft Word (они имеют расширение .DOC). Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманд. Как и для других типов вирусов, результат атаки может быть как относительно безобидным, так и разрушительным.

8.3. Методы защиты от компьютерных вирусов

Три рубежа защиты от компьютерных вирусов:

1. предотвращение поступления вирусов;
2. предотвращение вирусной атаки, если вирус все-таки поступил на компьютер;
3. предотвращение разрушительных последствий, если атака все-таки произошла.

Три метода реализации защиты:

1. программные методы защиты;
2. аппаратные методы защиты;
3. организационные методы защиты.

8.4. Методы защиты ценных данных

В вопросе защиты ценных данных часто используют бытовой подход: «болезнь лучше предотвратить, чем лечить».

К сожалению, именно бытовой подход и вызывает наиболее разрушительные последствия.

Создав бастионы на пути проникновения вирусов в компьютер, нельзя положиться на их прочность и остаться неготовым к действиям после разрушительной атаки.

К тому же **вирусная атака — далеко не единственная и даже не самая распространенная причина утраты важных данных.**

8.4. Методы защиты ценных данных

Существуют 3 причины утраты ценных данных

1. **программные сбои**, которые могут вывести из строя операционную систему,

2. **аппаратные сбои**, способные сделать жесткий диск неработоспособным,

3. **вероятность утраты компьютера** вместе с ценными данными в результате кражи, пожара или иного стихийного бедствия.

8.4. Методы защиты ценных данных

Поэтому создавать систему безопасности следует в первую очередь «с конца» — с предотвращения разрушительных последствий любого воздействия

будь то

1. **вирусная атака,**
2. **кража в помещении**
3. **или физический выход жесткого диска из строя.**

Надежная и безопасная работа с данными достигается только тогда, когда любое неожиданное событие, в том числе и полное физическое уничтожение компьютера, не приведет к катастрофическим последствиям.

8.4.1. Резервное копирование

Основным средством защиты информации является резервное копирование наиболее ценных данных.

В случае утраты информации по любой из вышеперечисленных причин жесткие диски переформатируют и подготавливают к новой эксплуатации.

На «чистый» отформатированный диск устанавливают операционную систему с дистрибутивного компакт-диска.

Затем под управлением операционной системы устанавливают все необходимое программное обеспечение, которое тоже берут с дистрибутивных носителей. Восстановление компьютера завершается восстановлением данных, которые берут с резервных носителей.

8.4.1. Резервное копирование

При резервировании данных следует отдельно сохранять все регистрационные и парольные данные для доступа к сетевым службам Интернета. Их не следует хранить на компьютере.

Резервные копии конфиденциальных данных сохраняют на внешних носителях, которые хранят в сейфах, желательно в отдельных помещениях. При разработке организационного плана резервного копирования учитывают необходимость создания не менее двух резервных копий, сохраняемых в разных местах. Между копиями осуществляют ротацию. Например, в течение недели.

При разработке организационного плана резервного копирования учитывают необходимость создания не менее двух резервных копий, сохраняемых в разных местах. Между копиями осуществляют ротацию. Например, в течение недели ежедневно копируют данные на носители резервного комплекта «А», а через неделю их заменяют комплектом «Б» и т. д.

8.4.2. Программные средства антивирусной защиты

Программные средства антивирусной защиты предоставляют следующие возможности.

1. **Создание образа жесткого диска на внешних носителях** . В случае выхода из строя данных в системных областях жесткого диска сохраненный «образ диска» может позволить восстановить если не все данные, то по крайней мере их большую часть. Это же средство может защитить от утраты данных при аппаратных сбоях и при неаккуратном форматировании жесткого диска.

2. **Регулярное сканирование жестких дисков в поисках компьютерных вирусов**. Сканирование обычно выполняется автоматически при каждом включении компьютера и при размещении внешнего диска в считывающем устройстве. При сканировании следует иметь в виду, что антивирусная программа ищет вирус путем сравнения кода программ с кодами известных ей вирусов, хранящимися в базе данных.
3. **Для надежной работы следует регулярно обновлять антивирусную программу.** Если база данных устарела, а вирус является новым, сканирующая программа его не обнаружит. Желательная периодичность обновления — один раз в две недели; допустимая — один раз в три месяца. Для примера укажем, что разрушительные последствия атаки вируса W95.CIH. 1075 («Чернобыль»), вызвавшего уничтожение информации на сотнях тысяч компьютеров 26 апреля 1999 года, были связаны не с

8.4.2. Программные средства антивирусной защиты

Программные средства антивирусной защиты предоставляют следующие возможности.

1. **Контроль изменения размера и других атрибутов файлов.** Поскольку некоторые компьютерные вирусы на этапе размножения изменяют параметры зараженных файлов, контролирующая программа может обнаружить их деятельность и предупредить пользователя.

2. **Контроль обращений к жесткому диску**. Поскольку наиболее опасные операции, связанные с работой компьютерных вирусов, так или иначе обращены на модификацию данных, записанных на жестком диске, антивирусные программы могут контролировать обращения к нему и предупреждать пользователя о подозрительной активности.

8.4.3. Защита информации в Интернете

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 пользователя 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

1. вольные или невольные попытки нарушить работоспособность компьютерных систем,
2. попытки взлома защищенных систем, использование и распространение программ, нарушающих работоспособность компьютерных систем (в частности, компьютерных вирусов).

.

8.4.3. Защита информации в Интернете

Работая во Всемирной сети, следует помнить

В Интернете 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.

8.4.3. Защита информации в Интернете

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.

Начиная с 1999 года Интернет становится мощным средством обеспечения розничного торгового оборота, а это требует защиты данных кредитных карт и других электронных платежных средств.

8.4.3. Принцип защиты информации в Интернете

Принципы защиты информации в Интернете опираются на определение информации, сформулированное нами в первой лекции.

Информация — это продукт взаимодействия данных и адекватных им методов.

Если в ходе коммуникационного процесса данные передаются через открытые системы (а Интернет относится именно к таковым), то исключить доступ к ним посторонних лиц невозможно даже теоретически.

Соответственно, **системы защиты** сосредоточены на втором компоненте информации — **на методах**.

Их принцип действия 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**.

8.5. Криптографические методы защиты информации

Понятие о симметричном шифровании информации

Системам шифрования столько же лет, сколько письменному обмену информацией. Симметричный метод шифрования основан на применении к шифруемому документу специального шифровального ключа, после чего документ становится недоступен для чтения обычными средствами. Его можно прочитать только тот, кто знает ключ, — только он может применить адекватный метод чтения. Аналогично происходит шифрование и ответного сообщения. **Если в процессе обмена информацией для шифрования и чтения пользуются одним и тем же ключом, то такой криптографический процесс является симметричным**.

Основной недостаток симметричного процесса заключается в том, что, прежде чем начать обмен информацией, надо выполнить передачу ключа, а для этого опять-таки нужна защищенная связь, то есть проблема повторяется, хотя и на другом уровне. Если рассмотреть оплату клиентом товара или услуги с помощью кредитной карты, то получается, что торговая фирма должна создать по одному ключу для каждого своего клиента и каким-то образом передать им эти ключи. Это крайне неудобно.

8.5. Криптографические методы защиты информации

Понятие о несимметричном шифровании информации

В настоящее время в Интернете используют несимметричные криптографические системы, основанные на использовании не одного, а двух ключей.

Происходит это следующим образом. Компания для работы с клиентами создает два ключа: один открытый (public — публичный), а другой закрытый (private —личный). На самом деле это как бы две «половинки» одного целого ключа, связанные друг с другом.

Ключи устроены так, что сообщение, зашифрованное одной половинкой, можно расшифровать только другой половинкой (не той, которой оно было закодировано). Создав пару ключей, торговая компания широко распространяет публичный ключ (открытую половинку) и надежно сохраняет закрытый ключ (свою половинку). Как публичный, так и закрытый ключи представляют собой некую кодовую последовательность. Публичный ключ компании может быть опубликован на ее сервере, откуда каждый желающий может его получить.

8.5. Криптографические методы защиты информации

Понятие о несимметричном шифровании информации

Если клиент хочет сделать фирме заказ, он возьмет ее публичный ключ и с его помощью закодирует свое сообщение о заказе и данные о своей кредитной карте. После кодирования это сообщение может прочесть только владелец закрытого ключа. Никто из участников цепочки, по которой пересылается информация, не в состоянии это сделать. Даже сам отправитель не может прочитать собственное сообщение, хотя ему хорошо известно содержание. Лишь получатель сможет прочесть сообщение, поскольку только у него есть закрытый ключ, дополняющий использованный публичный ключ.

Если фирме надо будет отправить клиенту квитанцию о том, что заказ принят к исполнению, она закодирует ее своим закрытым ключом. Клиент сможет прочитать квитанцию, воспользовавшись имеющимся у него публичным ключом данной фирмы. Он может быть уверен, что квитанцию ему отправила именно эта фирма, поскольку никто иной доступа к закрытому ключу фирмы не имеет.

8.5. Криптографические методы защиты информации

Принцип достаточности защиты

Защита публичным ключом (впрочем, как и большинство других видов защиты информации) не является абсолютно надежной.

Поскольку каждый желающий может получить и использовать чей-то публичный ключ, то он может сколь угодно подробно изучить алгоритм работы механизма шифрования и пытаться установить метод расшифровки сообщения, то есть реконструировать закрытый ключ. Это настолько справедливо, что алгоритмы кодирования публичным ключом даже нет смысла скрывать. Обычно к ним есть доступ, а часто они просто широко публикуются. Тонкость заключается в том, **что знание алгоритма еще не означает возможности провести реконструкцию ключа в разумно приемлемые сроки**.

Так, например, правила игры в шахматы известны всем, и нетрудно создать алгоритм для перебора всех возможных шахматных партий, но он никому не нужен, поскольку даже самый быстрый современный суперкомпьютер будет работать над этой задачей дольше, чем существует жизнь на нашей планете.

8.5. Криптографические методы защиты информации

Принцип достаточности защиты

Защиту информации принято считать достаточной, если затраты на ее преодоление превышают ожидаемую ценность самой информации.

В этом состоит принцип достаточности защиты, которым руководствуются при использовании несимметричных средств шифрования данных. Он предполагает, что защита не абсолютна и приемы ее снятия известны, но она все же достаточна для того, чтобы сделать это мероприятие нецелесообразным.

Разумеется, не всегда реконструкцию закрытого ключа производят методами простого перебора комбинаций. Для этого существуют специальные методы, основанные на исследовании особенностей взаимодействия открытого ключа с определенными структурами данных. Область науки, посвященная этим исследованиям, называется **криптоанализом**, а средняя продолжительность времени, необходимого для реконструкции закрытого ключа по его опубликованному открытому ключу, называется **криптостойкостью**

8.5. Криптографические методы защиты информации

Принцип достаточности защиты

Для многих методов несимметричного шифрования **криптостойкость**, полученная в результате криптоанализа, существенно отличается от величин, заявляемых разработчиками алгоритмов на основании теоретических оценок.

Поэтому во многих странах вопрос применения алгоритмов шифрования данных находится в поле законодательного регулирования.

В России к использованию в государственных и коммерческих организациях разрешены только те программные средства шифрования данных, которые прошли государственную сертификацию в административных органах, в частности, в Федеральном агентстве правительственной связи и информации при Президенте Российской Федерации (**ФАПСИ**).

8.6. Электронная подпись

Мы рассмотрели, как клиент может переслать организации свои конфиденциальные данные (например, номер электронного счета). Точно так же он может общаться и с банком, отдавая ему распоряжения о перечислении своих средств на счета других лиц и организаций. Ему не надо ездить в банк и стоять в очереди — все можно сделать, не отходя от компьютера. Однако здесь возникает проблема: как банк узнает, что распоряжение поступило именно от данного лица, а не от злоумышленника, выдающего себя за него? Эта проблема решается с помощью так называемой электронной подписи.

Принцип ее создания тот же, что и рассмотренный выше. Если нам надо создать себе электронную подпись, следует с помощью специальной программы (полученной от банка) создать те же два ключа: закрытый и публичный. Публичный ключ передается банку. Если теперь надо отправить поручение банку на операцию с расчетным счетом, оно кодируется публичным ключом банка, а своя подпись под ним кодируется собственным закрытым ключом. Банк поступает наоборот. Он читает поручение с помощью своего закрытого ключа, а подпись — с помощью публичного ключа поручителя. Если подпись читаема, банк может быть уверен, что

8.6. Электронная подпись

Мы рассмотрели, как клиент может переслать организации свои конфиденциальные данные (например, номер электронного счета). Точно так же он может общаться и с банком, отдавая ему распоряжения о перечислении своих средств на счета других лиц и организаций. Ему не надо ездить в банк и стоять в очереди — все можно сделать, не отходя от компьютера. Однако здесь возникает проблема: как банк узнает, что распоряжение поступило именно от данного лица, а не от злоумышленника, выдающего себя за него? Эта проблема решается с помощью так называемой электронной подписи.

Принцип ее создания тот же, что и рассмотренный выше. Если нам надо создать себе электронную подпись, следует с помощью специальной программы (полученной от банка) создать те же два ключа: закрытый и публичный. Публичный ключ передается банку. Если теперь надо отправить поручение банку на операцию с расчетным счетом, оно кодируется публичным ключом банка, а своя подпись под ним кодируется собственным закрытым ключом. Банк поступает наоборот. Он читает поручение с помощью своего закрытого ключа, а подпись — с помощью публичного ключа поручителя. Если подпись читаема, банк может быть уверен, что

На сегодня все…

Благодарю
за внимание !!!