Содержание:

Введение

Для подавляющего большинства компьютерных преступлений характерны корыстные мотивы. Однако представляет интерес наметившаяся в последнее время тенденция к совершению таких преступлений специалистами – профессиональными электронщиками или программистами. Люди, работающие в этой области, обычно весьма любознательны и обладают острым умом, а также склонностью к озорству. Они нередко воспринимают меры по обеспечению безопасности вычислительных (компьютерных) систем как вызов своему профессионализму и стараются найти технические пути, которые доказали бы их личное превосходство. Постепенно они не только набирают опыт, но и приобретают вкус к этой деятельности. В конце концов им приходит в голову мысль, что если уж заниматься такого рода “игрой”, то лучше одновременно получать и какую-то выгоду. Программисты рассчитывают поднять свой престиж, похвастaвшись перед знакомыми или коллегами умением найти слабости в компьютерной системе, а иногда и просто продемонстрировать, как эти слабости можно использовать.

Основная часть

Рассмотрим *основные виды компьютерных преступлений, связанных со злоумышленным нарушением ИБ*

I. Перехват информации.

1. *Непосредственный перехват.* Осуществляется, как правило, либо через телефонный канал системы, либо подключением к линии принтера.

2. *Электромагнитный перехват.* Не требует непосредственного подключения к системе и производится улавливанием с помощью специальных средств излучения, производимого центральным процессором, дисплеем, телефоном, принтером и др.

3. *“Жучок”.* Установка микрофона в компьютере с целью перехвата разговоров работающего на ЭВМ персонала.

4. *Откачивание данных.* Сбор информации, требующейся для получения основных материалов. Часто при этом исследуется не само содержание информации, а схемы ее движения.

5. *“Уборка мусора”:* 1) физический вариант – сбор использованных листингов, выброшенных служебных бумаг и т.д.; 2) электронный вариант – исследование данных, оставленных в памяти ЭВМ.

II. Несанкционированный доступ.

1. *“За дураком”:* 1) физический вариант – проникновение в помещения, где установлены компьютеры, следом за законным пользователем; 2) электронный вариант – подключение терминала незаконного пользователя к линии связи законного пользователя в начале работы или при прерывании активного режима.

2. *“За хвост”.* Перехват сигнала, обозначающего конец работы законного пользователя с последующим осуществлением доступа к системе.

3. *“Абордаж”.* Хакеры часто проникают в чужие информационные системы, подбирая номера на удачу, угадывая коды и т.п.

4. *“Неспешный выбор”.* Несанкционированный доступ к файлам законного пользователя осуществляется нахождением слабых мест в защите системы. Однажды обнаружив их, нарушитель может не спеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней многократно.

5. *“Брешь”.* В отличие от “неспешного выбора”, где ищутся слабые места в защите системы, при данном способе производится поиск брешей, обусловленных ошибками или неудачной логикой построения программы.

6. “*Люк*”. “Люк” – это развитие приема “брешь”. В найденной бреши программа “развивается”, и туда дополнительно вставляют одну или несколько команд. Люк “открывается” по мере необходимости, а встроенные команды автоматически осуществляют свою задачу.

7. *“Системные ротозеи”.* Расчет на неадекватную проверку полномочий пользователя (имена, коды, шифр-ключи и т. п.). Несанкционированный доступ осуществляется нахождением бреши в программе входа в систему.

8. *“Маскарад”:* 1) физический вариант – для получения информации злоумышленники выдают себя за других лиц, чаще всего за журналистов; 2) электронный вариант – проникновение в компьютерную систему по кодам и другим идентификационным шифрам законных пользователей.

9. *“Мистификация”.* Иногда случается, как например с ошибочным телефонными звонками, что пользователь удаленного терминала подключается к чьей-то системе, будучи абсолютно уверенным, что работает с той системой, с какой и намеревался. Владелец системы, к которой произошло фактическое подключение, формируя правдоподобные отклики, может поддерживать это заблуждение в течение определенного времени и получать некоторую информацию, в частности, коды доступа к данным.

10. *Аварийный доступ.* Используется тот факт, что в любом компьютерном комплексе имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ, – своеобразный аналог приспособлений, помещаемых в транспорте под надписью “Разбить стекло в случае аварии”. Такая программа – мощный и опасный инструмент в руках злоумышленника.

11. *“Склад без стен”.* Несанкционированный доступ осуществляется в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных. Все происходит так, словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что у нее нет одной стены.

III. Манипулирование данными.

1. *Подмена данных.* Изменение или введение ложных данных осуществляется, как правило, при вводе в ЭВМ или выводе истинных данных.

2. *Подмена кода.* Вариантом подмены данных является изменение кода программы.

3. *“Троянский конь”.* Тайное введение в чужую программу таких команд, которые позволяют осуществить новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность. По существу, это “люк”, который открывается не “вручную”, а автоматически, без дальнейшего участия злоумышленника. С помощью “троянского коня” преступники, например, могут отчислять на свой счет определенную сумму денег с каждой банковской операции.

4. *“Троянский конь в цепях”.* В отличие от программных “троянских коней”, которые представляют собой совокупность команд, речь идет о “троянских конях” в электронных цепях компьютеров. Это очень редкий способ, потому что если в предыдущих поколениях компьютеров, где использовались схемные соединения и печатные платы, еще можно было применять этот прием, то сейчас внести какие-либо изменения можно, пожалуй, только на уровне конструирования и заводского производства печатных плат.

5. *“Троянская матрешка”.* Еще одна разновидность “троянского коня”. Ее особенность состоит в том, что в программы вставляются не команды, выполняющие “грязную” работу, а команды, формирующие эти команды и после их выполнения уничтожающие их. В этом случае программисту, пытающемуся найти “троянского коня”, необходимо искать не его самого, а формирующие его команды.

6. *“Компьютерные вирусы”.* “Троянские кони”, обладающие способностью размножаться и выполнять вредоносные действия. Современные вирусы обладают свойством переходить в компьютерных сетях из одной вычислительной системы в другую, распространяясь, как вирусное заболевание.

7. *“Салями”.* Это способ использования “троянского коня” в сфере электронных банковских операций, основанный на том, что отчисляемые (на счет злоумышленника) суммы малы, а их потери практически незаметны (например по 1 коп. с операции). Накопление осуществляется за счет большого количества операций. Данный способ – один из простейших и безопасных способов, особенно если отчисляются дробные денежные суммы (стоимостью меньше, чем самая малая денежная единица, например 1 коп.), поскольку в этих случаях все равно делается округление.

8. *“Логическая бомба”.* Тайное встраивание в программу команд, которые должны сработать один раз или срабатывать многократно при определенных условиях.

9. *“Временная бомба”.* Разновидность “логической бомбы”, которая срабатывает в определенный момент времени.

10. *“Асинхронная атака”.* Сложный способ, требующий хорошего знания операционной системы. Используя асинхронную природу функционирования операционной системы, ее заставляют работать при ложных условиях, из-за чего управление обработкой информации частично или полностью нарушается. Если лицо, совершающее “асинхронную атаку”, достаточно искусно, оно может использовать ситуацию, чтобы внести изменения в операционную систему или

направить ее на выполнение своих целей, причем вне системы эти изменения не будут заметны.

11. *Моделирование*.

А. *Реверсивная модель.* Создается модель конкретной системы. В нее вводятся реальные исходные данные и учитываются планируемые действия. Затем, исходя из полученных правильных результатов, подбираются правдоподобные желаемые результаты. После этого модель возвращается назад, к исходной точке, и становится ясно, какие манипуляции с входными данными нужно проводить. В принципе “прокручивание” модели “вперед-назад” может происходить не один раз, чтобы через несколько итераций добиться желаемого результата. После этого остается только осуществить задуманное действие.

Б. *“Воздушный змей”.* В простейшем случае требуется открыть в двух банках по небольшому счету. Далее деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило извещение о переводе в этот банк, а общая сумма перевода соответствовала сумме первого перевода. Этот цикл повторяется большое число раз (“воздушный змей” поднимается все выше и выше) до тех пор, пока на счете не оказывается достаточно большая сумма (фактически она постоянно “перескакивает” с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются и владелец счетов исчезает. Этот способ требует очень точного расчета, но для двух банков его можно сделать и без компьютера. На практике в такую “игру” включают большое число банков, так что сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью компьютера.

В. *“Ловушка на живца”.* Создание особой программы, удачно разрекламированной и потому якобы представляющей интерес для специалистов (“живец”). На самом деле эта программа работает некоторое время, затем имитирует системную поломку и записывает коды доступа в систему всех пользователей, осуществляющих работу с нею. Полученные данные используются для других компьютерных злоупотреблений.

Заключение

Перечисленные компьютерные преступления чаще всего представляют собой: хищение денег (подделка счетов и платежных ведомостей, приписка сверхурочных часов работы, фальсификация платежных документов, вторичное получение уже произведенных выплат, перечисление денег на подставные счета и т.д.); хищение вещей (совершение покупок с фиктивной оплатой, добывание запасных частей и редких материалов); хищение машинной информации; внесение изменений в машинную информацию; несанкционированную эксплуатацию системы; несанкционированное использование ресурсов ЭВМ или сети (например, хищение машинного времени); подделку документов (полученных фальшивых дипломов, фиктивное продвижение по службе); саботаж; шпионаж (политический, военный и промышленный).

Особым видом компьютерного преступления является вандализм, который обычно принимает форму физического разрушения вычислительных (компьютерных) систем или их компонентов. Часто этим занимаются уволенные сотрудники из чувства мести, люди, страдающие компьютерными фобиями.