Компьютеры: преступления, признаки уязвимости и меры защиты

Содержание

Введение

Меры защиты: четыре уровня защиты

Признаки компьютерных преступлений

Информационная безопасность

Преступления и злоупотребления

Пять основных технологий, использовавшихся при совершении компьютерных преступлений

## Введение

Информационная Эра привела к драматическим изменениям в способе выполнения своих обязанностей для большого числа профессий. Теперь нетехнический специалист среднего уровня может выполнять работу, которую раньше делал высококвалифицированный программист. Служащий имеет в своем распоряжении столько точной и оперативной информации, сколько никогда не имел.

Но использование компьютеров и автоматизированных технологий приводит к появлению ряда проблем для руководства организацией. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным. Все увеличивается число компьютерных преступлений, что может привести в конечном счете к подрыву экономики. И поэтому должно быть ясно, что информация - это ресурс, который надо защищать.

Ответственность за защиту информации лежит на низшем звене руководства. Но также кто-то должен осуществлять общее руководство этой деятельностью, поэтому в организации должно иметься лицо в верхнем звене руководства, отвечающее за поддержание работоспособности информационных систем.

И так как автоматизация привела к тому, что теперь операции с вычислительной техникой выполняются простыми служащими организации, а не специально подготовленным техническим персоналом, нужно, чтобы конечные пользователи знали о своей ответственности за защиту информации.

Число компьютерных преступлений растет - также увеличиваются масштабы компьютерных злоупотреблений. По оценке специалистов США, ущерб от компьютерных преступлений увеличивается на 35 процентов в год и составляет около 3.5 миллиардов долларов. Одной из причин является сумма денег, получаемая в результате преступления: в то время как ущерб от среднего компьютерного преступления составляет 560 тысяч долларов, при ограблении банка - всего лишь 19 тысяч долларов.

Шансов быть пойманным у компьютерного преступника гораздо меньше, чем у грабителя банка - и даже при поимке у него меньше шансов попасть в тюрьму. Обнаруживается в среднем 1 процент компьютерных преступлений. И вероятность того, что за компьютерное мошенничество преступник попадет в тюрьму, меньше 10 процентов.

Умышленные компьютерные преступления составляют заметную часть преступлений. Но злоупотреблений компьютерами и ошибок еще больше. Как выразился один эксперт, "мы теряем из-за ошибок больше денег, чем могли бы украсть". Эти потери подчеркивают важность и серьезность убытков, связанных с компьютерами.

Основной причиной наличия потерь, связанных с компьютерами, является недостаточная образованность в области безопасности. Только наличие некоторых знаний в области безопасности может прекратить инциденты и ошибки, обеспечить эффективное применение мер защиты, предотвратить преступление или своевременно обнаружить подозреваемого. Осведомленность конечного пользователя о мерах безопасности обеспечивает четыре уровня защиты компьютерных и информационных ресурсов:

## Меры защиты: четыре уровня защиты

***Предотвращение*** *- только авторизованный персонал имеет доступ к информации и технологии*

***Обнаружение*** *- обеспечивается раннее обнаружение преступлений и злоупотреблений, даже если механизмы защиты были обойдены*

***Ограничение -*** *уменьшается размер потерь, если преступление все-таки произошло несмотря на меры по его предотвращению и обнаружению.*

***Восстановление*** *- обеспечивается эффективное восстановление информации при наличии документированных и проверенных планов по восстановлению*

Вчера контроль за технологией работы был заботой технических администраторов. Сегодня контроль за информацией стал обязанностью каждого нетехнического конечного пользователя. Контроль за информацией требует новых знаний и навыков для группы нетехнических служащих. Хороший контроль за информацией требует понимания возможностей совершения компьютерных преступлений и злоупотреблений, чтобы можно было в дальнейшем предпринять контрмеры против них.

Когда компьютеры впервые появились, они были доступны только небольшому числу людей, которые умели их использовать. Обычно они помещались в специальных помещениях, удаленных территориально от помещений, где работали служащие. Сегодня все изменилось. Компьютерные терминалы и настольные компьютеры используются везде. Компьютерное оборудование стало дружественным к пользователю, поэтому много людей могут быстро и легко научиться тому, как его использовать.

Число служащих в организации, имеющих доступ к компьютерному оборудованию и информационной технологии, постоянно растет.д.оступ к информации больше не ограничивается только узким кругом лиц из верхнего руководства организации. Этот процесс привел к тому, что произошла "демократизация преступления". Чем больше людей получало доступ к информационной технологии и компьютерному оборудованию, тем больше возникало возможностей для совершения компьютерных преступлений.

Трудно обобщать, но теперь компьютерным преступником может быть...

конечный пользователь, не технический служащий и не хакер

тот, кто не находится на руководящей должности

тот, у кого нет судимостей

умный, талантливый сотрудник

тот, кто много работает

тот, кто не разбирается в компьютерах

тот, кого вы подозревали бы в последнюю очередь

именно тот, кого вы взяли бы на работу

КОМПЬЮТЕРНЫМ ПРЕСТУПНИКОМ МОЖЕТ БЫТЬ ЛЮБОЙ.

Типичный компьютерный преступник - это не молодой хакер, использующий телефон и домашний компьютер для получения доступа к большим компьютерам. Типичный компьютерный преступник - это служащий, которому разрешен доступ к системе, нетехническим пользователем которой он является. В США компьютерные преступления, совершенные служащими, составляют 70-80 процентов ежегодного ущерба, связанного с компьютерами. Остальные 20 процентов дают действия нечестных и недовольных сотрудников. И совершаются они по целому ряду причин.

***ПОЧЕМУ ЛЮДИ СОВЕРШАЮТ КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ:***

личная или финансовая выгода,

развлечение,

месть,

попытка добиться расположения кого-либо к себе,

самовыражение,

случайность,

вандализм.

Но значительно больший ущерб, около 60 процентов всех потерь, наносят ошибки людей и инциденты. Предотвращение компьютерных потерь, как из-за умышленных преступлений, так и из-за неумышленных ошибок, требует знаний в области безопасности. Опросы, проводимые периодически в США, показывают, что именно служащие, имевшие знания в области компьютерной безопасности, были основной причиной выявления компьютерных преступлений.

## Признаки компьютерных преступлений

Обращайте внимание на:

неавторизованное использование компьютерного времени,

неавторизованные попытки доступа к файлам данных,

кражи частей компьютеров,

кражи программ,

физическое разрушение оборудования,

уничтожение данных или программ,

неавторизованное владение дискетами, лентами или распечатками.

И это только самые очевидные признаки, на которые следует обратить внимание при выявлении компьютерных преступлений. Иногда эти признаки говорят о том, что преступление уже совершено, или что не выполняются меры защиты. Они также могут свидетельствовать о наличии уязвимых мест - указать, где находится дыра в защите - и помочь наметить план действий по устранению уязвимого места. В то время как признаки могут помочь выявить преступление или злоупотребление - меры защиты могут помочь предотвратить его.

Меры защиты - это меры, вводимые руководством, для обеспечения безопасности информации - административные руководящие документы (приказы, положения, инструкции), аппаратные устройства или дополнительные программы - основной целью которых является предотвратить преступления и злоупотребления, не позволив им произойти. Меры защиты могут также выполнять функцию ограничения, уменьшая размер ущерба от преступления.

## Информационная безопасность

То, что в 60-е годы называлось компьютерной безопасностью, а в 70-е - безопасностью данных, сейчас более правильно именуется информационной безопасностью. Информационная безопасность подчеркивает важность информации в современном обществе - понимание того, что информация - это ценный ресурс, нечто большее, чем отдельные элементы данных.

**Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе**. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода. Целью информационной безопасности является обезопасить ценности системы, защитить и гарантировать точность и целостность информации, и минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, в ходе которых информация создается, модифицируется, к ней обеспечивается доступ или она распространяется.

Информационная безопасность дает гарантию того, что достигаются следующие цели:

конфиденциальность критической информации

целостность информации и связанных с ней процессов (создания, ввода, обработки и вывода)

доступность информации, когда она нужна

учет всех процессов, связанных с информацией

Некоторые технологии по защите системы и обеспечению учета всех событий могут быть встроены в сам компьютер. Другие могут быть встроены в программы. Некоторые же выполняются людьми и являются реализацией указаний руководства, содержащихся в соответствующих руководящих документах. Принятие решения о выборе уровня сложности технологий для защите системы требует установления критичности информации и последующего определения адекватного уровня безопасности.

Что же такое критические данные? ***Под критическими данными будем понимать данные, которые требуют защиты из-за вероятности нанесения (риска) ущерба и его величины в том случае, если произойдет случайное или умышленное раскрытие, изменение, или разрушение данных.*** Этот термин включает в себя данные, чье неправильное использование или раскрытие может отрицательно отразиться на способности организации решать свои задачи, персональные данные и другие данные, защита которых требуется указами Президента РФ, законами РФ и другими подзаконными документами.

## ****Преступления и злоупотребления****

Анализ зарубежных и отечественных отчетов о выявленных компьютерных преступлениях позволяет описать основные технологии их совершения. Лишь немногие из них включают разрушение компьютеров или данных. Только в 3 процентах мошенничеств и 8 процентах злоупотреблений происходило специальное разрушение оборудования, уничтожение программ или данных. В большей части случаев мошенничеств и злоупотреблений использовалась информация - ею манипулировали, ее создавали, ее использовали.

## Пять основных технологий, использовавшихся при совершении компьютерных преступлений

**Мошенничества:**

Ввод неавторизованной информации

Манипуляции разрешенной для ввода информацией

Манипуляции или неправильное использование файлов с информацией

Создание неавторизованных файлов с информацией

Обход внутренних мер защиты

**Злоупотребления:**

Кража компьютерного времени, программ, информации и оборудования

Ввод неавторизованной информации

Создание неавторизованных файлов с информацией

Разработка компьютерных программ для неслужебного использования

Манипулирование или неправильное использование возможностей по проведению работ на компьютерах

С другой стороны стоит рассмотреть основные методы, использовавшиеся для их совершения. Они включают:

**Надувательство с данными.** Наверное, самый распространенный метод при совершении компьютерных преступлений, так как он не требует технических знаний и относительно безопасен. Информация меняется в процессе ее ввода в компьютер или во время вывода. Например, при вводе документы могут быть заменены фальшивыми, вместо рабочих дискет подсунуты чужие, и данные могут быть сфальсифицированы.

**Сканирование.** Другой распространенный метод получения информации, который может привести к преступлению. Служащие, читающие файлы других, могут обнаружить там персональную информацию о своих коллегах. Информация, позволяющая получить доступ к компьютерным файлам или изменить их, может быть найдена после просмотра мусорных корзин. Дискеты, оставленные на столе, могут быть прочитаны, скопированы, и украдены. Очень хитрый сканирующий может даже просматривать остаточную информацию, оставшуюся на компьютере или на носителе информации после выполнения сотрудником задания и удаления своих файлов.

**Троянский конь.** Этот метод предполагает, что пользователь не заметил, что компьютерная программа была изменена таким образом, что включает в себя дополнительные функции. Программа, выполняющая полезные функции, пишется таким образом, что содержит дополнительные скрытые функции, которые будут использовать особенности механизмов защиты системы (возможности пользователя, запустившего программу, по доступу к файлам)

**Люк.** Этот метод основан на использовании скрытого программного или аппаратного механизма, позволяющего обойти методы защиты в системе. Этот механизм активируется некоторым неочевидным образом. Иногда программа пишется таким образом, что специфическое событие, например, число транзакций, обработанных в определенный день, вызовет запуск неавторизованного механизма.

**Технология салями.** Названа так из-за того, что преступление совершается понемногу, небольшими частями, настолько маленькими, что они незаметны. Обычно эта технология сопровождается изменением компьютерной программы. Например, платежи могут округляться до нескольких центов, и разница между реальной и округленной суммой поступать на специально открытый счет злоумышленника.

**Суперотключение**. Названа по имени программы, использовавшейся в ряде компьютерных центров, обходившей системные меры защиты и использовавшейся при аварийных ситуациях. Владение этим "мастер-ключом" дает возможность в любое время получить доступ к компьютеру и информации, находящейся в нем.

Три принятии решений администраторы ИС сталкиваются с проблемой выбора вариантов решений по организации ЗИ на основе учета принципов деятельности организации, соотношения важности целей и наличия ресурсов. Эти решения включают определение ого, как будут защищаться технические и информационные ресурсы, а также как должны вести себя служащие в тех или иных ситуациях.

Политика информационной безопасности - набор законов, правил, практических рекомендаций и практического опыта, определяющих управленческие и проектные решения в области ЗИ. На основе ПИБ строится управление, защита и распределение критичной информации в системе. Она должна охватывать все особенности процесса обработки информации, определяя поведение ИС в различных ситуациях.

В соответствии с предложенным в книге подходом олитика (МЕРЫ) информационной безопасности 303) реализуется соответствующей СТРУКТУРОЙ органов (002) на основе нормативно-методической АЗЫ (001) с использованием программно-технических методов и СРЕДСТВ (004), определяющих архитектуру системы защиты.

Для конкретной ИС политика безопасности должна быть индивидуальной. Она зависит от технологии обработки информации, используемых программных и технических средств, структуры организации и т.д.

Следует рассматривать такие направления защиты ИС:

010 Защита объектов информационной системы;

020 Защита процессов, процедур и программ обработки информации;

030 Защита каналов связи;

040 Подавление побочных электромагнитных излучений;

050 Управление системой защиты.

Очевидно, что каждое из указанных НАПРАВЛЕНИЙ должно быть детализировано в зависимости от особенностей структуры ИС.

Кроме этого ПИБ должна описывать следующие ЭТАПЫ создания СЗИ:

100 Определение информационных и технических ресурсов, подлежащих защите;

200 Выявление полного множества потенциально возможных угроз и каналов утечки информации;

300 Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;

400 Определение требований к системе защиты;

500 Осуществление выбора средств защиты информации и их характеристик;

600 Внедрение и организация использования выбранных мер, способов и средств защиты;

700 Осуществление контроля целостности и управление системой защиты.

**Принципы политики безопасности (003).**

Политика безопасности определяется как совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами:

1. Невозможность миновать защитные средства;

2. Усиление самого слабого звена;

3. Недопустимость перехода в открытое состояние;

4. Минимизация привилегий;

5. Разделение обязанностей;

6. Многоуровневая защита;

7. Разнообразие защитных средств;

8. Простота и управляемость информационной системы;

9. Обеспечение всеобщей поддержки мер безопасности.