Содержание:

ВВЕДЕНИЕ :

В кодексе Российской федерации , статья 272 , которая гласит о –

1. неправомерном доступе к охраняемой законом компьютерной информации , если это деяние повлекло уничтожение , блокирование , модификацию либо копирование компьютерной информации , наказывается штрафом в размере двухсот тысяч рублей или в размере заработанной платы или иного дохода осужденного за период до восемнадцати месяцев , либо исправительными работами на срок до одного года , может даже быть ограничение свободы на срок до двух лет , так же может быть лишение свободы на такой же срок – двух лет.
2. возможно тоже деяние , причинившее крупный ущерб или совершенное из корыстной заинтересованности и т. д

Сейчас в наше время идет огромное развитие новых информационных технологий . Все это привело к тому что , информационная безопасность , становится не только

обязательной , она еще одна из характеристик ИС.
ИС- информационная система
Под безопасностью ИС понимается защищенность систем от случайных или преднамеренного вмешательства в естественный процесс ее функционирования , от попыток хищения информации. Если говорить простыми словами , способность противодействия различным возмущающим воздействиям на ИС.
Под *угрозой безопасности информации* понимаются события или действия, которые могут привезти к искажению использованию информации не по уголовному кодексу Р.Ф
Среди угроз безопасности информации следует выделять как один из видов угрозы **случайные , или непредсказуемые** . Их источником могут быть выход из строя аппаратных средств , неправильные действия работников ИС или ее пользователей , непреднамеренные ошибки в программном обеспечении тд

Такие угрозы , так же следует держать в внимании , так как их ущерб может быть весьма значительным , Однако в этой главе больше всего стоит уделять внимание конечном *умышленным* , которые , в отличие от случайных , преследуют цель нанесения ущерба управляемой системе или тем же самым пользователям . Это делается достаточно часто , для своей личной выгоды. Человека , пытающегося нарушить работу информационной системы или получить несанкционированный доступ к информации , обычно называют ВЗЛОМЩИКОМ , а иногда «компьютерным пиратом»(хакером).

ВИДЫ УМЫШЛЕНЫХ УГРОЗ БЕЗОПАСТНОСТИ ИНФОРМАЦИИ

Пассивные угрозы - направлены в основном на несанкционированное использование информационных ресурсов ИС, не оказывая при этом влияния на ее функционирование. Например , несанкционированный доступ к базам данным , прослушивающие каналы и так далее.
Активные угрозы- имеют цель цель нарушения нормального функционирования ИС путем целенаправленного воздействия на ее так сказать компоненты.

К активным угрозам относятся , например вывод из строя компьютеры или его оператора , разрушение програмного обеспечения компьютеров , нарушения работы линий связи и так далее .

Так же есть *умышленные угрозы* , о они подразделяются на два вида

1. Внутренние
2. Внешние

Внутренние угрозы , чаще всего определяются социальной напряженностью

Внешние угрозы могут определяться злонамеренными действиями конкурентов экономическими условиями и другими причинами.

К основным угрозам безопасности информации и нормального функционирования ИС относятся:

• утечка конфиденциальной информации;

• компрометация информации;

• несанкционированное использование информационных ресурсов;

• ошибочное использование информационных ресурсов;

• несанкционированный обмен информацией между абонентами;

• отказ от информации;

• нарушение информационного обслуживания;

• незаконное использование привилегий.

Утечка конфиденциальной информации — это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы. Эта утечка может быть следствием:

• разглашения конфиденциальной информации;

• ухода информации по различным, главным образом техническим, каналам;

• несанкционированного доступа *к* конфиденциальной информации различны-ми способами.

Наиболее распространенными путями несанкционированного доступа к информации являются:

• перехват электронных излучений;

• принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей;

• применение подслушивающих устройств (закладок);

• дистанционное фотографирование;

• перехват акустических излучений и восстановление текста принтера;

• копирование носителей информации с преодолением мер защиты

• маскировка под зарегистрированного пользователя;

• маскировка под запросы системы;

• использование программных ловушек;

• использование недостатков языков программирования и операционных систем;

• незаконное подключение к аппаратуре и линиям связи специально разработанных аппаратных средств, обеспечивающих доступ информации;

• злоумышленный вывод из строя механизмов защиты;

• расшифровка специальными программами зашифрованной: информации;

• информационные инфекции.

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Создание систем информационной безопасности **(СИБ)** в ИС и ИТ основывается на следующих принципах:

Системный подход к построению системы защиты, означающий оптимальное сочетание взаимосвязанных организационных, программных,аппаратных, физических и других свойств, подтвержденных практикой создания отечественных и зарубежных систем защиты и применяемых на всех этапах технологического цикла обработки информации.

Принцип непрерывного развития системы. Этот принцип, являющийся одним из основополагающих для компьютерных информационных систем, еще более актуален для СИБ. Способы реализации угроз информации в ИТ непрерывно совершенствуются, а потому обеспечение безопасности ИС не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования СИБ, непрерывном контроле, выявлении ее узких и слабых мест, потенциальных каналов утечки информации и новых способов несанкционированного доступа,

Обеспечение надежности системы защиты, т. е. невозможность снижения уровня надежности при возникновении в системе сбоев, отказов, преднамеренных действий взломщика или непреднамеренных ошибок пользователей и обслуживающего персонала.

Обеспечение контроля за функционированием системы защиты, т.е. создание средств и методов контроля работоспособности механизмов защиты.

Обеспечение всевозможны средств борьбы с вредоносными программами.

Обеспечение экономической целесообразности использования системы. защиты, что выражается в превышении возможного ущерба ИС и ИТ от реализации угроз над стоимостью разработки и эксплуатации СИБ.

В результате решения проблем безопасности информации современные ИС и ИТ должны обладать следующими основными признаками:

• наличием информации различной степени конфиденциальности;

• обеспечением криптографической защиты информации различной степени конфиденциальности при передаче данных;

• обязательным управлением потоками информации, как в локальных сетях, так и при передаче по каналам связи на далекие расстояния;

• наличием механизма регистрации и учета попыток несанкционированного доступа, событий в ИС и документов, выводимых на печать;

• обязательным обеспечением целостности программного обеспечения и информации в ИТ;

• наличием средств восстановления системы защиты информации; • обязательным учетом магнитных носителей;

• наличием физической охраны средств вычислительной техники и магнитных носителей;

• наличием специальной службы информационной безопасности системы.

Методы и средства обеспечения безопасности информации:

Препятствие — метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом — методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации. Управление

доступом включает следующие функции защиты:

• идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);

• опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

• разрешение и создание условий работы в пределах установленного регламента;

• регистрацию (протоколирование) обращений к защищаемым ресурсам;

• реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

Механизмы шифрования — криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке, так и при хранении информации на магнитных носителях.

Противодействие атакам вредоносных программ предполагает комплекс разнообразных мер организационного характера и использование антивирусных программ.

Вся совокупность технических средств подразделяется на аппаратные и физические.

Аппаратные средства — устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие *защиту* персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. Примеры физических средств:

замки на дверях, решетки на окнах, средства электронной охранной сигнализации и т.п.

Программные средства — это специальные программы и программные комплексы, предназначенные для защиты информации в ИС.

Из средств ПО системы защиты необходимо выделить еще программные средства, реализующие механизмы шифрования (криптографии),

Криптография — это наука об обеспечении секретности или аутентичности (подлинности) передаваемых сообщений.

Организационные средства осуществляют своим комплексом регламентацию производственной деятельности в ИС и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ *к* конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты включают всевозможные нормы поведения, которые традиционно сложились ранее, складываются по мере распространения ИС и ИТ в стране и в мире или специально разрабатываются. Морально-этические нормы могут быть неписаные (например, честность) либо оформленные в некий свод (устав) правил или предписаний. Эти нормы, как правило, не являются законодательно утвержденными, но поскольку их несоблюдение приводит к падению престижа организации, они считаются обязательными для исполнения.

Криптографические методы защиты информации

Готовое к передаче информационное сообщение, первоначально открытое и незащищенное, зашифровывается и тем самым преобразуется в шифрограмму, т. е. в закрытые текст или графическое изображение документа. В таком виде сообщение передается по каналу связи, даже и не защищенному. Санкционированный пользователь после получения сообщения дешифрует его (т. е. раскрывает) посредством обратного преобразования криптограммы, вследствие чего получается исходный, открытый вид сообщения, доступный для восприятия санкционированным пользователям.

Методу преобразования в криптографической системе соответствует использование специального алгоритма. Действие такого алгоритма запускается уникальным числом, обычно называемым шифрующим ключом.

Современная криптография знает два типа криптографических алгоритмов: классические алгоритмы, основанные на использовании закрытых, секретных ключей, и новые алгоритмы с открытым ключом, в которых используются один открытый и один закрытый ключ (эти алгоритмы называются также асимметричными). Кроме того, существует возможность шифрования информации и более простым способом — с использованием генератора псевдослучайных чисел.

Использование генератора псевдослучайных чисел заключается в генерации гаммы шифра с помощью генератора псевдослучайных чисел при определенном ключе и наложении полученной гаммы на открытые данные обратимым способом.

Надежность шифрования с помощью генератора псевдослучайных чисел зависит как от характеристик генератора, так и, причем в большей степени, от алгоритма получения гаммы.

Этот метод криптографической защиты реализуется достаточно легко и обеспечивает довольно высокую скорость шифрования, однако недостаточно стоек к дешифрованию и поэтому неприменим для таких серьезных информационных систем, каковыми являются, например, банковские системы.

Для классической криптографии характерно использование одной секретной единицы — ключа, который позволяет отправителю зашифровать сообщение, а получателю расшифровать его. В случае шифрования данных, хранимых на магнитных или иных носителях информации, ключ позволяет зашифровать информацию при записи на носитель и расшифровать при чтении с него.

Наиболее перспективными системами криптографической защиты данных сегодня считаются асимметричные криптосистемы, называемые также системами с открытым ключом. Их суть состоит в том, что ключ, используемый для зашифровывания, отличен от ключа расшифровывания. При этом ключ зашифровывания не секретен и может быть известен всем пользователям системы. Однако расшифровывание с помощью известного ключа зашифровывания невозможно. Для расшифровывания используется специальный, секретный ключ. Знание открытого ключа не позволяет определить ключ секретный. Таким образом, расшифровать сообщение может только его получатель, владеющий этим секретным ключом.

Известно несколько криптосистем с открытым ключом. Наиболее разработана на сегодня система RSA. RSA— это система коллективного пользования, в которой каждый из пользователей имеет свои ключи зашифровывания и расшифровывания данных, причем секретен только ключ расшифровывания.

Специалисты считают, что системы с открытым ключом больше подходят для шифрования передаваемых данных, чем для защиты данных, хранимых на носителях информации. Существует еще одна область применения этого алгоритма — цифровые подписи, подтверждающие подлинность передаваемых документов и сообщений.

Из изложенного следует, что надежная криптографическая система должна удовлетворять ряду определенных требований.

• Процедуры зашифровывания и расшифровывания должны быть «прозрачны» для пользователя.

• Дешифрование закрытой информации должно быть максимально затруднено.

• Содержание передаваемой информации не должно сказываться на эффективности криптографического алгоритма.

Процессы защиты информации, шифрования и дешифрования связаны с кодируемыми объектами и процессами, их свойствами, особенностями перемещения. Такими объектами и процессами могут быть материальные объекты, ресурсы, товары, сообщения, блоки информации, транзакции (минимальные взаимодействия с базой данных по сети). Кодирование кроме целей защиты, повышая скорость доступа к данным, позволяет быстро определять и выходить на любой вид товара и продукции, страну-производителя и т.д. В единую логическую цепочку связываются операции, относящиеся к одной сделке, но географически разбросанные по сети.

Например, штриховое кодирование используется как разновидность автоматической идентификации элементов материальных потоков, например товаров, и применяется для контроля за их движением в реальном времени. Достигается оперативность управления потоками материалов и продукции, повышается эффективность управления предприятием. Штриховое кодирование позволяет не только защитить информацию, но и обеспечивает высокую скорость чтения и записи кодов. Наряду со штриховыми кодами в целях защиты информации используют голографические методы.

Методы защиты информации с использованием голографии являются актуальным и развивающимся направлением. Голография представляет собой раздел науки и техники, занимающийся изучением и созданием способов, устройств для записи и обработки волн различной природы. Оптическая голография основана на явлении интерференции волн. Интерференция волн наблюдается при распределении в пространстве волн и медленном пространственном распределении результирующей волны. Возникающая при интерференции волн картина содержит информацию об объекте. Если эту картину фиксировать на светочувствительной поверхности, то образуется голограмма. При облучении голограммы или ее участка опорной волной можно увидеть объемное трехмерное изображение объекта. Голография применима к волнам любой природы и в настоящее время находит все большее практическое применение для идентификации продукции различного назначения.

Технология применения кодов в современных условиях преследует цели защиты информации, сокращения трудозатрат и обеспечение быстроты ее обработки, экономии компьютерной памяти, формализованного описания данных на основе их систематизации и классификации.

В совокупности кодирование, шифрование и защита данных предотвращают искажения информационного отображения реальных производственно-хозяйственных процессов, движения материальных, финансовых и других потоков, а тем самым способствуют обоснованности формирования и принятия управленческих решений.

ЗАКЛЮЧЕНИЕ:

Информация давно перестала быть просто необходимым для производства вспомогательным ресурсом или побочным проявлением всякого рода деятельности. Она приобрела ощутимый стоимостный вес, который четко определяется реальной прибылью, получаемой при ее использовании, или размерами ущерба, с разной степенью вероятности наносимого владельцу информации. Создание индустрии переработки информации порождает целый ряд сложных проблем. Одной из таких проблем является надежное обеспечение сохранности и установленного статуса информации, циркулирующей и обрабатываемой в информационно-вычислительных системах и сетях.

Можно сказать, что не существует одного абсолютно надежного метода защиты. Наиболее полную безопасность можно обеспечить только при комплексном подходе к этому вопросу. Необходимо постоянно следить за новыми решениями в этой области. В крупных организациях я бы рекомендовала ввести должность специалиста по информационной безопасности.