Батаева И.П.
Пензенский государственный университет

ЗАЩИТА ИНФОРМАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость в том, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Так постепенно защита экономической информации становится обязательной: разрабатываются всевозможные документы по защите информации; формируются рекомендации по защите информации; даже проводится федеральный закон о защите информации, который рассматривает проблемы защиты информации и задачи защиты информации, а также решает некоторые уникальные вопросы защиты информации.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

На сегодняшний день существует широкий круг систем хранения и обработки информации, где в процессе их проектирования фактор информационной безопасности Российской Федерации хранения конфиденциальной информации имеет особое значение. К таким информационным системам можно отнести, например, банковские или юридические системы безопасного документооборота и другие информационные системы, для которых обеспечение защиты информации является жизненно важным для защиты информации в информационных системах.

Под информационной безопасностью Российской Федерации (информационной системы) подразумевается техника защиты информации от преднамеренного или случайного несанкционированного доступа и нанесения тем самым вреда нормальному процессу документооборота и обмена данными в системе, а также хищения, модификации и уничтожения информации [1].

Другими словами вопросы защиты информации в информационных системах решаются для того, чтобы изолировать нормально функционирующую информационную систему от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения.

Под фразой «угрозы безопасности информационных систем» понимаются реальные или потенциально возможные действия или события, которые способны исказить хранящиеся в информационной системе данные, уничтожить их или использовать в каких-либо целях, не предусмотренных регламентом заранее.

Если взять модель, описывающую любую управляемую информационную систему, можно предположить, что возмущающее воздействие на нее может быть случайным. Именно поэтому, рассматривая угрозы безопасности информационных систем, следует сразу выделить преднамеренные и случайные возмущающие воздействия.

Комплекс защиты информации может быть выведен из строя, например из-за дефектов аппаратных средств. Также вопросы защиты информации встают ребром благодаря неверным действиям персонала, имеющего непосредственный доступ к базам данных, что влечет за собой снижение эффективности защиты информации при любых других благоприятных условиях проведения мероприятия по защите информации. Кроме этого в программном обеспечении могут возникать непреднамеренные ошибки и другие сбои информационной системы. Все это негативно влияет на эффективность защиты информации любого вида информационной безопасности, который существует и используется в информационных системах.

Защита информации от компьютерных вирусов (защита информации в информационных системах) предполагает средства защиты информации в сети, а точнее программно аппаратные средства защиты информации, которые предотвращают несанкционированное выполнение вредоносных программ, пытающихся завладеть данными и выслать их злоумышленнику, либо уничтожить информацию базы данных, но защита информации от компьютерных вирусов неспособна в полной мере отразить атаку хакера или человека, именуемого компьютерным пиратом.

Задача защиты информации и защиты информации от компьютерных вирусов заключается в том, чтобы усложнить или сделать невозможным проникновение, как вирусов, так и хакера к секретным данным, ради чего взломщики в своих противоправных действиях ищут наиболее достоверный источник секретных данных. А так как хакеры пытаются получить максимум достоверных секретных данных с минимальными затратами, то задачи защиты информации - стремление запутать злоумышленника: служба защиты информации предоставляет ему неверные данные, защита компьютерной информации пытается максимально изолировать базу данных от внешнего несанкционированного вмешательства и т.д.

Защита компьютерной информации для взломщика – это те мероприятия по защите информации, которые необходимо обойти для получения доступа к сведениям. Архитектура защиты компьютерной информации строится таким образом, чтобы злоумышленник столкнулся с множеством уровней защиты информации: защита сервера посредством разграничения доступа и системы аутентификации (диплом «защита информации») пользователей и защита компьютера самого пользователя, который работает с секретными данными. Защита компьютера и защита сервера одновременно позволяют организовать схему защиты компьютерной информации таким образом, чтобы взломщику было невозможно проникнуть в систему, пользуясь столь ненадежным средством защиты информации в сети, как человеческий фактор. То есть, даже обходя защиту компьютера пользователя базы данных и переходя на другой уровень защиты информации, хакер должен будет правильно воспользоваться данной привилегией, иначе защита сервера отклонит любые его запросы на получение данных и попытка обойти защиту компьютерной информации окажется тщетной [2].

Публикации последних лет говорят о том, что техника защиты информации не успевает развиваться за числом злоупотреблений полномочиями, и техника защиты информации всегда отстает в своем развитии от технологий, которыми пользуются взломщики для того, чтобы завладеть чужой тайной.

Существуют документы по защите информации, описывающие циркулирующую в информационной системе и передаваемую по связевым каналам информацию, но документы по защите информации непрерывно дополняются и совершенствуются, хотя и уже после того, как злоумышленники совершают все более технологичные прорывы модели защиты информации, какой бы сложной она не была.

Сегодня для реализации эффективного мероприятия по защите информации требуется не только разработка средства защиты информации в сети и разработка механизмов модели защиты информации, а реализация системного подхода или комплекса защиты информации – это комплекс взаимосвязанных мер, описываемый определением «защита информации». Данный комплекс защиты информации, как правило, использует специальные технические и программные средства для организации мероприятий защиты экономической информации.

Кроме того, модели защиты информации предусматривают ГОСТ «Защита информации», который содержит нормативно-правовые акты и морально-этические меры защиты информации, и противодействие атакам извне. ГОСТ «Защита информации» нормирует определение защиты информации рядом комплексных мер

защиты информации, которые проистекают из комплексных действий злоумышленников, пытающихся любыми силами завладеть секретными сведениями. И сегодня можно смело утверждать, что постепенно ГОСТ и определение защиты информации рождают современную технологию защиты информации в сетях компьютерных информационных системах и сетях передачи данных, как диплом «защита информации».

Какие сегодня существуют виды информационной безопасности и умышленных угроз безопасности информации

Виды информационной безопасности, а точнее виды угроз защиты информации на предприятии подразделяются на пассивную и активную.

Пассивный риск информационной безопасности направлен на внеправовое использование информационных ресурсов и не нацелен на нарушение функционирования информационной системы. К пассивному риску информационной безопасности можно отнести, например, доступ к базам данных или прослушивание каналов передачи данных.

Активный риск информационной безопасности нацелен на нарушение функционирования действующей информационной системы путем целенаправленной атаки на ее компоненты.

К активным видам угрозы компьютерной безопасности относится, например, физический вывод из строя компьютера или нарушение его работоспособности на уровне программного обеспечения.

Необходимость средств защиты информации. Системный подход к организации защиты информации от несанкционированного доступа

К методам и средствам защиты информации относят организационно-технические и правовые мероприятия информационной защиты и меры защиты информации (правовая защита информации, техническая защита информации, защита экономической информации и т.д.).

Организационные методы защиты информации и защита информации в России обладают следующими свойствами [3]:

Методы и средства защиты информации обеспечивают частичное или полное перекрытие каналов утечки согласно стандартам информационной безопасности (хищение и копирование объектов защиты информации);

Система защиты информации - это объединенный целостный орган защиты информации, обеспечивающий многогранную информационную защиту;

Методы и средства защиты информации и основы информационной безопасности включают в себя:

Безопасность информационных технологий, основанная на ограничении физического доступа к объектам защиты информации с помощью режимных мер и методов информационной безопасности;

Информационная безопасность организации и управление опирается на разграничение доступа к объектам защиты информации - это установка правил разграничения доступа органами защиты информации, шифрование информации для ее хранения и передачи (криптографические методы защиты информации, программные средства защиты информации и защита информации в сетях);

Информационная защита должна обязательно обеспечить регулярное резервное копирование наиболее важных массивов данных и надлежащее их хранение (физическая защита информации);

Органы защиты информации должны обеспечивать профилактику заражение компьютерными вирусами объекта защиты информации.

Правовые основы защиты информации и закон о защите информации. Защита информации на предприятии

Правовые основы защиты информации - это законодательный орган защиты информации, в котором можно выделить до 4 уровней правового обеспечения информационной безопасности информации и информационной безопасности предприятия [3].

Первый уровень правовой охраны информации и защиты состоит из международных договоров о защите информации и государственной тайны, к которым присоединилась и Российская Федерация с целью обеспечения надежной информационной безопасности РФ. Кроме того, существует доктрина информационной безопасности РФ, поддерживающая правовое обеспечение информационной безопасности нашей страны.

Правовое обеспечение информационной безопасности весьма на высоком уровне, и многие компании могут рассчитывать на полную экономическую информационную безопасность и правовую охрану информации, и защиту, благодаря федеральному закону о защите информации.

На втором уровне правовой охраны информации и защиты (ФЗ о защите информации) - это подзаконные акты: указы Президента РФ и постановления Правительства, письма Высшего Арбитражного Суда и постановления пленумов ВС РФ.

Третий уровень правового обеспечения системы защиты экономической информации.

К данному уровню обеспечения правовой защиты информации относятся ГОСТы безопасности информационных технологий и обеспечения безопасности информационных систем.

Также на третьем уровне безопасности информационных технологий присутствуют руководящие документы, нормы, методы информационной безопасности и классификаторы, разрабатывающиеся государственными органами.

Четвертый уровень стандарта информационной безопасности защиты конфиденциальной информации образуют локальные нормативные акты, инструкции, положения и методы информационной безопасности и документация по комплексной правовой защите информации рефераты по которым часто пишут студенты, изучающие технологии защиты информации, компьютерную безопасность и правовую защиту информации.

Проблемы информационной безопасности в сфере технической защиты информации [4]:

Перехват электронных излучений. Проблема решается обеспечением защиты информации, передаваемой по радиоканалам связи и обмена данными информационной системы;

Принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей. Проблема решается с помощью инженерной защитой информацией или физическая защита информации, передаваемой по связевым кабельным линиям передачи данных. Сюда также относится защита информации в локальных сетях, защита информации в интернете и технические средства информационной безопасности;

применение подслушивающих устройств;

дистанционное фотографирование, защита информации реферат;

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.

Вышеперечисленные пути утечки информации по оценке информационной безопасности требуют высокого уровня технических знаний для того чтобы использовать наиболее эффективные методы и системы защиты информации, кроме этого необходимо обладать высоким уровнем аппаратных и программных средств защиты информации, так как взломщик, охотящийся за ценными сведениями, не пожалеет средств для того, чтобы обойти защиту и безопасность информации системы. Например, физическая защита информации предотвращает использование технических каналов утечки данных к злоумышленнику. Причина, по которой могут появиться подобные «дыры» - конструктивные и технические дефекты решений защиты информации от несанкционированного доступа, либо физический износ элементов средств обеспечения информационной безопасности. Это дает возможность взломщику устанавливать преобразователи, которые образуют некие принципы действующего канала передачи данных, и способы защиты информации должны предусматривать и идентифицировать подобные «жучки».

Средства обеспечения информационной безопасности от вредоносного программного обеспечения (ПО)

К сожалению, Закон о защите информации работает только в случае, когда нарушитель чувствует и может понести ответственность за несанкционированный обход службы защиты информации. Однако, сегодня существует и постоянно создается гигантское количество вредоносного и шпионского ПО, которое преследует целью порчу информации в базах данных и, хранящихся на компьютерах документов. Огромное количество разновидностей таких программ и их постоянное пополнение рядов не дает возможности раз и навсегда решить проблемы защиты информации и реализовать универсальную систему программно аппаратной защиты информации, пригодной для большинства информационных систем.

Вредоносное программное обеспечение, направленное на нарушение системы защиты информации от несанкционированного доступа можно классифицировать по следующим критериям:

Логическая бомба используется для уничтожения или нарушения целостности информации, однако, иногда ее применяют и для кражи данных. Логическая бомба является серьезной угрозой, и информационная безопасность предприятия не всегда способна справиться с подобными атаками, ведь манипуляциями с логическими бомбами пользуются недовольные служащие или сотрудники с особыми политическими взглядами, то есть, информационная безопасность предприятия подвергается не типовой угрозе, а непредсказуемой атаке, где главную роль играет человеческий фактор. Например, есть реальные случаи, когда предугадавшие свое увольнение программисты вносили в формулу расчета зарплаты сотрудников компании корректировки, вступающие в силу сразу после того, как фамилия программиста исчезает из перечня сотрудников фирмы. Как видите, ни программные средства защиты информации, ни физическая защита информации в этом случае на 100% сработать не может. Более того, выявить нарушителя и наказать по всей строгости закона крайне сложно, поэтому правильно разработанная комплексная защита информации способна решить проблемы защиты информации в сетях [5].

Троянский конь – это программа, запускающаяся к выполнению дополнительно к другим программным средствам защиты информации и прочего ПО, необходимого для работы.

То есть, троянский конь обходит систему защиты информации путем завуалированного выполнения недокументированных действий.

Такой дополнительный командный блок встраивается в безвредную программу, которая затем может распространяться под любым предлогом, а встроенный дополнительный алгоритм начинает выполняться при каких-нибудь заранее спрогнозированных условиях, и даже не будет замечен системой защиты информации, так как защита информации в сетях будет идентифицировать действия алгоритма, работой безвредной, заранее документированной программы. В итоге, запуская такую программу, персонал, обслуживающий информационную систему подвергает опасности компанию. И опять виной всему человеческий фактор, который не может на 100% предупредить ни физическая защита информации, ни любые другие методы и системы защиты информации.

Вирус - это специальная самостоятельная программа, способная к самостоятельному распространению, размножению и внедрению своего кода в другие программы путем модификации данных с целью бесследного выполнения вредоносного кода. Существует специальная защита информации от вирусов!

Обеспечение безопасности информационных систем от вирусных атак традиционно заключается в использовании такой службы защиты информации, как антивирусное ПО и сетевые экраны. Эти программные решения позволяют частично решить проблемы защиты информации, но, зная историю защиты информации, легко понять, что установка системы защиты коммерческой информации и системы защиты информации на предприятии на основе антивирусного ПО сегодня еще не решает проблему информационной безопасности общества завтра. Для повышения уровня надежности системы и обеспечения безопасности информационных систем требуется использовать и другие средства информационной безопасности, например, организационная защита информации, программно аппаратная защита информации, аппаратная защита информации.

Вирусы характеризуются тем, что они способны самостоятельно размножаться и вмешиваться в вычислительный процесс, получая возможность управления этим процессом.

То есть, если Ваша программно аппаратная защита информации пропустила подобную угрозу, то вирус, получив доступ к управлению информационной системой, способен автономно производить собственные вычисления и операции над хранящейся в системе конфиденциальной информацией.

Наличие паразитарных свойств у вирусов позволяет им самостоятельно существовать в сетях сколь угодно долго до их полного уничтожения, но проблема обнаружения и выявления наличия вируса в системе до сих пор не может носить тотальный характер, и ни одна служба информационной безопасности не может гарантировать 100-процентную защиту от вирусов, тем более, что информационная безопасность государства и любой другой способ защиты информации контролируется людьми.

Червь - программа, передающая свое тело или его части по сети. Не оставляет копий на магнитных носителях и использует все возможные механизмы для передачи себя по сети и заражения атакуемого компьютера. Рекомендацией по защите информации в данном случае является внедрение большего числа способов защиты информации, повышение качества программной защиты информации, внедрение аппаратной защиты информации, повышение качества технических средств защиты информации и в целом развитие комплексной защиты информации информационной системы.

Перехватчик паролей – программный комплекс для воровства паролей и учетных данных в процессе обращения пользователей к терминалам аутентификации информационной системы.

Программа не пытается обойти службу информационной безопасности напрямую, а лишь совершает попытки завладеть учетными данными, позволяющими не вызывая никаких подозрений совершенно санкционировано проникнуть в информационную систему, минуя службу информационной безопасности, которая

ничего не заподозрит. Обычно программа инициирует ошибку при аутентификации, и пользователь, думая, что ошибся, при вводе пароля, повторяет ввод учетных данных и входит в систему, однако, теперь эти данные становятся известны владельцу перехватчика паролей, и дальнейшее использование старых учетных данных небезопасно.

Важно понимать, что большинство краж данных происходят не благодаря хитроумным способам, а из-за небрежности и невнимательности, поэтому понятие информационной безопасности включает в себя: информационную безопасность (лекции), аудит информационной безопасности, оценка информационной безопасности, информационная безопасность государства, экономическая информационная безопасность и любые традиционные и инновационные средства защиты информации.

Защита информации и информационная безопасность строится на следующих принципах:

построение системы информационной безопасности в России, также как и информационной безопасности организации требует к себе системного подхода, который предполагает оптимальную пропорцию между организационных, программных, правовых и физических свойств информационной безопасности РФ, подтвержденной практикой создания средств защиты информации по методам защиты информации, применимых на любом этапе цикла обработки информации системы;

непрерывность развития системы управления информационной безопасностью. Для любой концепции информационной безопасности, тем более, если используются методы защиты информации в локальных сетях и компьютерных системах, принцип непрерывного развития является основополагающим, ведь информационная безопасность информации постоянно подвергается все новым и новым с каждым разом еще более изощренным атакам, поэтому обеспечение информационной безопасности организации не может быть разовым актом, и созданная однажды технология защиты информации, будет постоянно совершенствоваться вслед за ростом уровня взломщиков;

принцип обеспечения надежности системы защиты информации и информационная безопасность – это невозможность снижения уровня надежности системы во время сбоев, отказов, ошибок и взломов (Защита информации – курсовая работа);

обязательно необходимо обеспечить контроль и управление информационной безопасностью, для отслеживания и регулирования механизмов защиты;

обеспечение средств борьбы с вредоносным ПО. Например, всевозможные программы для защиты информации и система защиты информации от вирусов;

экономическая целесообразность использования системы защиты информации и государственной тайны. Целесообразность построения системы защиты экономической информации заключается в превышении суммы ущерба при взломе системы защиты информации на предприятии над стоимостью разработки средства защиты компьютерной информации, защиты банковской информации и комплексной защиты информации.

Одним из методов защиты информации является создание физической преграды пути злоумышленникам к защищаемой информации (если она хранится на каких-либо носителях).

Управление доступом – эффективный метод защиты информации, регулирующий использование ресурсов информационной системы, для которой разрабатывалась концепция информационной безопасности.

Методы и системы защиты информации, опирающиеся на управление доступом, включают в себя следующие функции защиты информации в локальных сетях информационных систем:

идентификация пользователей, ресурсов и персонала системы информационной безопасности сети;

опознание и установление подлинности пользователя по вводимым учетным данным (на данном принципе работает большинство моделей информационной безопасности);

допуск к определенным условиям работы согласно регламенту, предписанному каждому отдельному пользователю, что определяется средствами защиты информации и является основой информационной безопасности большинства типовых моделей информационных систем;

протоколирование обращений пользователей к ресурсам, информационная безопасность которых защищает ресурсы от несанкционированного доступа и отслеживает некорректное поведение пользователей системы. (Написать реферат средства защиты информации);

информационная безопасность банков и экономическая информационная безопасность и других систем должна обеспечивать своевременное реагирование на попытки несанкционированного доступа к данным посредством сигнализации, отказов и задержке в работе.

ЛИТЕРАТУРА

1. Мельников,В.П.Информационная безопасность и защита информации. / В.П.Мельников, С.А.Клейменов, А.М.Петраков // 3-е изд., стер. - М.: Академия, 2008. — 336 с.

2. Черней, Г.А. Безопасность автоматизированных информационных систем. / Г. А. Черней, С. А. Охрименко, Ф. С. Ляху // Ruxanda,1996. – 225 с.

3. Галатенко, В.А. Основы информационной безопасности.

4. Варлатая, С.К. Аппаратно-программные средства и методы защиты информации. / С.К. Варлатая, М.В.Шаханова // Владивосток: Изд-во ДВГТУ, 2007. - 318 с.

5. Корнюшин, П.Н., Костерин А.С. Информационная безопасность. / П.Н. Корнюшин, А.С. Костерин // Владивосток: ТИДОТ ДВГУ, 2003. - 154 с.