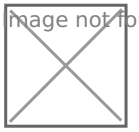
Содержание:



Введение

Хорошо известно, что в современном мире информация имеет определенную, а часто и очень высокую ценность. Как и любую ценность ее нужно защищать. Защита необходима, например, от потерь из-за случайного удаления, сбоев, вирусов, несанкционированного доступа к информации.

Под мероприятиями по защите от несанкционированного доступа имеются в виду те, что связаны с секретностью информации. К их числу относятся самые разнообразные способы защиты, начиная от простейших, но очень эффективных защит паролем до использования сложнейших технических систем. Как показывает практика, вероятность взлома современных средств защиты информации гораздо ниже, чем вероятность доступа к секретной информации в их обход. Поэтому особое внимание следует обращать не только на системы защиты, но и на различные организационные вопросы – подбор людей, допускаемых к секретной информации, тщательное соблюдение правил работы с ней и т.д.

На сегодняшнее время никакая система защиты не обеспечивает стопроцентную надежность. Достаточно надежной считается такая система защиты информации, которая обеспечивает ее защиту в течении необходимого периода времени. Иными словами, система защита информации должна быть такой, чтобы на ее взлом потребовалось больше времени, чем время, которое эта информация должна оставаться секретной.

Многие знают, что существуют различные способы защиты информации. А от чего, и от кого её надо защищать? И как это правильно сделать? На эти и другие вопросы я в своей контрольной работе и постараюсь ответить.

Цель: Выявление источников угрозы информации и определение способов защиты от них.

Задачи: Выявить основные источники угрозы информации. Описать способы защиты. Дать рекомендации по использованию этих программ.

1.

2. 1. Защита информации и информационная безопасность

Появление новых информационных технологий и развитие мощных компьютерных

2. Методы защиты информации

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.

Другими словами вопросы защиты информации и 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. *Первое разделение угрозы безопасности информационных систем на виды*

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 (курсовая защита 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.

В этом разделе рассматривается умышленная угроза защиты информации, которая отличается от случайной угрозы защиты информации тем, что злоумышленник нацелен на нанесение ущерба системе и ее пользователям, и зачастую угрозы безопасности информационных систем – это не что иное, как попытки получения личной выгоды от владения конфиденциальной информацией.

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.

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 (реферат на тему защита 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 (защита информации) и определение защиты информации рождают современную технологию защиты информации в сетях компьютерных информационных системах и сетях передачи данных, как диплом «защита информации».

2.1.Виды информационной безопасности и умышленные угрозы.

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 БД 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 угроз 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:

• 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 информационной безопасностью 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.

3. Программно-технические средства

3.1.Средства обеспечения информационной безопасности от вредоносного программного обеспечения.

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.

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

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.

3.2. Криптография

– это наука, которая изучает и описывает модель информационной безопасности данных. Криптография открывает решения многих проблем информационной безопасности сети: аутентификация, конфиденциальность, целостность и контроль взаимодействующих участников.

Термин «Шифрование» означает преобразование данных в форму, не читабельную для человека и программных комплексов без ключа шифрования-расшифровки. Криптографические методы защиты информации дают средства информационной безопасности, поэтому она является частью концепции информационной безопасности.

Криптографическая защита информации (конфиденциальность)

Цели защиты информации в итоге сводятся к обеспечению конфиденциальности информации и защите информации в компьютерных системах в процессе передачи информации по сети между пользователями системы.

Защита конфиденциальной информации, основанная на криптографической защите информации, шифрует данные при помощи семейства обратимых преобразований, каждое из которых описывается параметром, именуемым «ключом» и порядком, определяющим очередность применения каждого преобразования.

Важнейшим компонентом криптографического метода защиты информации является ключ, который отвечает за выбор преобразования и порядок его выполнения. Ключ – это некоторая последовательность символов, настраивающая шифрующий и дешифрующий алгоритм системы криптографической защиты информации. Каждое такое преобразование однозначно определяется ключом, который определяет криптографический алгоритм, обеспечивающий защиту информации и информационную безопасность информационной системы.

Один и тот же алгоритм криптографической защиты информации может работать в разных режимах, каждый из которых обладает определенными преимуществами и недостатками, влияющими на надежность информационной безопасности России и средства информационной безопасности.

Основы информационной безопасности криптографии (Целостность данных)

Защита информации в локальных сетях и технологии защиты информации наряду с конфиденциальностью обязаны обеспечивать и целостность хранения информации. То есть, защита информации в локальных сетях должна передавать данные таким образом, чтобы данные сохраняли неизменность в процессе передачи и хранения.

Для того чтобы информационная безопасность информации обеспечивала целостность хранения и передачи данных необходима разработка инструментов, обнаруживающих любые искажения исходных данных, для чего к исходной информации придается избыточность.

Информационная безопасность в России с криптографией решает вопрос целостности путем добавления некой контрольной суммы или проверочной комбинации для вычисления целостности данных. Таким образом, снова модель информационной безопасности является криптографической – зависящей от ключа. По оценке информационной безопасности, основанной на криптографии, зависимость возможности прочтения данных от секретного ключа является наиболее надежным инструментом и даже используется в системах информационной безопасности государства.

Как правило, аудит информационной безопасности предприятия, например, информационной безопасности банков, обращает особое внимание на вероятность успешно навязывать искаженную информацию, а криптографическая защита информации позволяет свести эту вероятность к ничтожно малому уровню. Подобная служба информационной безопасности данную вероятность называет мерой имитостойкости шифра, или способностью зашифрованных данных противостоять атаке взломщика.

3.3. Экранирование

Экран (фаерволл, брэндмауер) - это средство разграничения доступа клиентов из одного множества к серверам из другого множества. Экран выполняет свои функции, контролируя все информационные потоки между двумя множествами систем.

В простейшем случае экран состоит из двух механизмов, один из которых ограничивает перемещение данных, а второй, наоборот, ему способствует. В более общем случае экран или полупроницаемую оболочку удобно представлять себе как последовательность фильтров. Каждый из них может задержать данные, а может и сразу "перебросить" их "на другую сторону". Кроме того, допускаются передача порции данных на следующий фильтр для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю.

Помимо функций разграничения доступа экраны осуществляют также протоколирование информационных обменов.

Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования формулируется как защита внутренней области от потенциально враждебной внешней. Так, межсетевые экраны устанавливают для защиты локальной сети организации, имеющей выход в открытую среду, подобную Internet. Другой пример экрана - устройство защиты порта, контролирующее доступ к коммуникационному порту компьютера до и после независимо от всех прочих системных защитных средств.

Экранирование позволяет поддерживать доступность сервисов внутренней области, уменьшая или вообще ликвидируя нагрузку, индуцированную внешней активностью. Уменьшается уязвимость внутренних сервисов безопасности, поскольку первоначально сторонний злоумышленник должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно и жестко. Кроме того, экранирующая система, в отличие от универсальной, может быть устроена более простым и, следовательно, более безопасным образом.

Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима конфиденциальности.

Важным понятием экранирования является зона риска, определяемая как множество систем, которые становятся доступными злоумышленнику после преодоления экрана или какого-либо из его компонентов. Для повышения надежности защиты, экран реализуют как совокупность элементов, так что "взлом"

одного из них еще не открывает доступ ко всей внутренней сети. Экранирование и с точки зрения сочетания с другими сервисами безопасности, и с точки зрения внутренней организации использует идею многоуровневой защиты, за счет чего внутренняя сеть оказывается в пределах зоны риска только в случае преодоления злоумышленником нескольких, по-разному организованных защитных рубежей. Экранирование может использоваться как сервис безопасности не только в сетевой, но и в любой другой среде, где происходит обмен сообщениями.

Экранирование - один из наиболее действенных способов защиты информации, но в бочке мёда обязательно найдётся ложка дёгтя, хотя я бы даже сказал 50 ложек дёгтя. Дело в том, что большинство межсетевых экранов требуют для своей полноценной и корректной работы административных прав. А ведь очень много экранов имеют уязвимости. Воспользовавшись одной из таких уязвимостей хакер без труда получит права, под которыми работает экран и соответственно станет супер пользователем в данной системе.

В более-менее развитых сетях под экран выделяют отдельный компьютер, который в свою очередь может выполнять роль не только межсетевого фильтра, но и маршруторизатора.

Часто экран представлен в виде программного пакета, но также экраны бывают представлены и в аппаратном виде. Такие фаерволлы справляются со своими функциям куда лучше своих программных собратьев. Они могут обрабатывать намного больше информации (следственно на них тяжело вызвать ошибку отказа в обслуживании), а также имеют меньше уязвимостей и больше возможностей. Соответственно, они стоят гораздо дороже брэндмауэров, реализуемых на программном уровне.

Заключение

В заключении хотелось бы подчеркнуть, что никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в компьютерных сетях.

В вычислительной технике понятие безопасности является весьма широким. Оно подразумевает и надежность работы компьютера, и сохранность ценных данных, и защиту информации от внесения в нее изменений неуполномоченными лицами, и сохранение тайны переписки в электронной связи. Разумеется, во всех

цивилизованных странах на безопасности граждан стоят законы, но в вычислительной технике правоприменительная практика пока не развита, а законотворческий процесс не успевает за развитием технологий, и надежность работы компьютерных систем во многом опирается на меры самозащиты.

Итак, можно привести массу фактов, свидетельствующих о том, что угроза информационному ресурсу возрастает с каждым днем, подвергая в панику ответственных лиц в банках, на предприятиях и в компаниях во всем мире.

Список использованной литературы

Фролов А. В, Фролов Г. В Осторожно: компьютерные вирусы. М. 2003.

Информатика под, ред. Черноскутовой И.А. Учебное пособие 2005-272 с.

Терехов А.В, Чернышев А.В, Чернышев В.Н. Учебное пособие ТГТУ 2007-128 с.

Информатика под ред. Хубаева Г.Н. Учебное пособие 2010-288 с.