Содержание:

ВВЕДЕНИЕ

В настоящее время во всех сферах общественной жизни бурно развиваются информационные технологии. Всё чаще информация станосится дорогостоящим товаром, производительной силой и стратегическими ресурсами государства. Как и любой иной ныне существующий товар, информация тоже должна оставаться в сохранности под надёжной защитой.

Обусловленность уязвимости информации в компьютерных системах заключается в её территориальной рассредоточенности, большой концетрацией вычислительных ресурсов, одновременным доступом к ресурсам компьютерных сетей многочисленных пользователей, долговременным хранением больших объёмов данных. Ежедневно на свет появляются новые угрозы, такие как: несанкционированные вмешательства или сетевые атаки, из-за этого, сколько бы времени не проходило, а острота проблемы информационной безопасности не уменьшается, а напротив, становится всё актуальней.

Предметная область информационной безопасности рассматривает такие вопросы, как: средства и методы защиты информации, политика информационной безопасности, классификация и анализ угроз безопасности, управление методами защиты информации.

В изучении таких дисциплин, как «Информатика» важное место занимает проблема информационной безопасности. Потому что без особого внимания к вопросам о защите информации не имеет смысла применение информационных технологий. Острую нужду обеспечения защиты информации в компьютерных системах вызывает наличие множества угроз, таких как: борьба государств в области информационных технологий или острое стремление криминальных структур к незаконному использованию информационных ресурсов. При этом ущерб от нарушения или даже отсутстсвия информационной безопасности приводит к особо крупным финансовым затратам.

Объектом изучения данной курсовой работы являются виды и составы угроз информационной безопасности. В связи с этим, основной целью этой работы будет попытка собрать информацию об информационной безопасности, угрозах,

средствах и методах борьбы с ними, что входят в предметную область изучаемого объекта.

Задача данной работы – охарактеризовать основные виды угроз, определить сущность информационной безопасности, рассмореть имеющиеся на данный момет средства и методы защиты инеформации.

Информационной базой курсовой работы будут являться учебные пособия, статьи журналов, учебники, литературные издания по соответствующей теме.

1. Понятие информационной безопасности

Необходимость решения комплексной проблемы защиты информации возникла сразу после создания массового информационного пространства и внедрения персональных компьютеров и компьютерных систем в массы.

Защита информации в компьютерных системах есть ничто иное, как систематическое использование методов и средств, принятие мер и реализация мероприятий с целью системного обеспечения требуемой надёжности информации, которая хранится и обрабатывается, используя средства. Объектом защиты может предстать как носитель или информация, так и информационный процесс, которому необходимо обеспечить защиту согласно послевленной цели защиты информации. Охрана компьютерной информации включает в себя меры отслеживания и устранение несанкционированного доступа неавторизованных лиц, уничтожения, повреждения, искажения, неправомерного использования, блокирования информации в формах и носителях, которые связаны именно с компьютерными технологиями и средствами хранения, копирования, передачи, обработки и доступа. Для того, чтобы обеспечить безопасность информации в компьютерных системах, необходима защита: технических средств передачи и обработки данных; инфармационных массивов, которые представлены в разных мащинных носителях, програмных средств, которые реализуют соответстующие методы, пользователей, технологию и алгоритмы обработки информации.

Информационной безопасностью называют защищённость информации от незаконного преобразования, ознакомления и уничтожения, а также защищённость информации и информационных ресурсов от атак, которые направлены на нарушение их стабильности работы. Информационной безопасности можно достичь обеспечивая конфиденциальность, достоверность данных, которые обрабатываются, их целостность, а также целостность и доступность ресурсов

компьютерных систем и информационных компонентов.

Доступность – это свойство информации, которое характеризует способность предоставить беспрепятственный и своевременный доступ пользователям к необходимой им инфомарции.

Конфиденциальность – это свойство, которое указывает на вынужденное введение ограничений доступа к тем или иным данным для определённого круга лиц. Иначе говоря, это обеспечивает гарантию того, что во время передачи данные станут известны лишь только разрешённым пользователям.

Достоверность – это свойство информации, которое выражается в строгой принадлежности субъекту, являющийся её источником, или же тому субъекту, который предоставил информацию.

Целостность – это свойство информации сохранять своё содержание или структуру в процессе хранения и передачи в неизменном виде по отношению к обусловленному фиксированному состоянию. Данные может изменять, создавать или вовсе уничтожать лишь авторизированное лицо.

Информационная безопасность может быть достигнута тем, что руководство соответствующего уровня проводит политику информационной безопасности. Один из основных документов, на основе которого проводится политика информационной безопасности, представляет из себя программу информационной безопасности. Данный документ разрабатывается высшими огранами управления государством, организацией, ведомством, как официальный документ. В данном документе описываются первостепенные направления решения задач защиты информации в компьютерных системах, а так же цели политики информационной безопасности. Также в программах информационной безопасности содержатся принципы построения систем защиты данных в компьютерных системах и общие требования.

2. Угрозы информационной безопасности

2.1 Понятие и классификация угроз информационной безопасности

Для обеспечения эффективной защиты информации в первую очередь требуется анализ и рассмотрение всех факторов, которые представляют какую-либо угрозу информационной безопасности.

Обычно под угрозой информационной безопасности компьютерной системы понимается потенциально возможный процесс, событие, действие или явление, оказывающее нежелательное воздействие на системы и данные, хранящиеся и обрбатывающиеся в них. Угрозы, подобные этим, влияя на данные через компоненты компьютерных систем, способны привести к копированию, искажению, уничтожению, блокированию или ограничению доступа к ней, незаконному распространению информации. В настоящий момент известен довольно широкий перечень угроз, которые разделяют по нескольким признакам.

По природе возникновения различают:

- естественные угрозы, которые вызваны влиянием на компьютерные системы стихийных природных явлений или объективных физических процессов;
- искусственные угрозы, которые вызваны деятельностью человека.

По степени преднамеренности проявления различают преднамеренные и случайные угрозы безопасности.

По непосредственному источнику угроз. Источники угроз представляют собой:

- человек. К примеру, разглашение конфиденциальной информации;
- природная среда. К примеру, стихийные бедствия;
- несанкционированные программно-аппаратные средства. К примеру, заражение компьютера вирусами;
- санкционированные программно-аппаратные средства. К примеру, отказ в работе операционной системы.

По положению источника угроз. Расположение источника угроз может представлять собой:

- непосредственно в компьютерной системе. К примеру, неправильное использование ресурсов;
- в пределах контролируемой зоны компьютерных систем. К примеру, кража носителей информации;
- вне контролируемой зоны компьютерных систем. К примеру, перехват информации, которая передаётся по каналам связи.

По степени воздействия на компьютерные системы различают:

- активные угрозы, вносящие изменения в содержание и структуру компьютерной системы;
- пассивные угрозы, неспособные при реализании ничего изменить в собержании и структуре компьютерной системы.

По этапам доступа программ или пользователей к ресурсам компьютерной системы:

- угрозы, появляющиеся на этапе доступа к ресурсам компьютерной системы;
- угрозы, которые могут проявиться после разрешения доступа.

По текущему месту расположения информации в компьютерной системе:

- угроза доступа к данным, которые циркулируют в линиях связи;
- угроза доступа к данным в оперативной памяти;
- угроза доступа к данным на внешних запоминающих устройствах. К примеру, копирование данных с жёсткого диска.

По способу доступа к ресурсам компьютерной системы:

- угрозы, которые используют скрытый неочевидный путь доступа к ресурсам компьютерной системы в обход сущетсвующих средств защиты;
- угрозы, которые используют прямой стандартный путь доступа к данным с помощью паролей, которые были получены незаконно или путём несанкционированного использования терминалов авторизированных пользователей.

По степени зависимости от активности компьютерной системы:

- угрозы, которые появляются лишь в процессе обработки информации;
- угрозы, которые повяляются независимо от активности работы компьютерной системы.

2.2 Виды угроз безопасности

Все множество потенциальных угроз безопасности информации в компьютерной системе может быть разделено на 2 основных класса, как показано в приложении 1.

Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют случайными или непреднамеренными. Механизм реализации случайных угроз в целом достаточно хорошо изучен, накоплен значительный опыт противодействия этим угрозам.

Виды угроз, не связанные с преднамеренными действиями злоумышленников и реализующиеся в случайные моменты времени, называют непреднамеренными или случайными.

Аварии и стихийные бедствия опасны тем, что они приносят разрушительные последствия для компьютерных систем. Доступ к данным станосится невозможен или же информация вовсе утрачивается из-за того, что компьютерные системы уязвимы к физическим разрушениям.

Отказы в работе и сбои особо сложных систем неизбежны. В результате таких сбоев и отказов системы искажаются или уничтожаются информация и программы, нарушается алгоритм работы устройств, нарушается работоспособность технических средств.

Ошибки при разработке компьютерной системы, программные или алгоритмические ошибки приводят к последствиям, которые аналогичны последствиям отказов или сбоев технических средств. Кроме этого, такие ошибки могут посодействовать злоумышленникам в проникновении и воздействии на ресурсы компьютерных систем.

К нарушению безопасности в 65% случаев приводят ошибки обслуживающего персонала и ошибки простых пользователей. К нарушению или уничтожению целостности конфиденциальной информации приводит небрежное, невнимательное, некомпетентное выполнение функциональных обязанностей сотрудниками или пользователями.

Преднамеренные угрозы тесно связаны с точечно направленными действиями нарушителей. Такой класс угрозы тяжело контролировать, он плохо изучен, достаточно динамичен и с каждым днём пополняется новыми угрозами.

Средства и методы диверсий и шпионажа зачастую используют для получения данных о системе защиты с целью взлома и проникновения в компьютерные системы. Кроме этого подобные угрозы используются и для уничтожения и хищения информационных ресурсов. К таким методам относятся визуальное наблюдение, подслушивание, поджоги, анализ и сбор отходов машинных носителей информации, кража документов и физических носителей информации,

подслушивание, кража атрибутов и программ системы защиты.

Несанкционированный доступ к информации обычно осуществляется с использованием типичных программных и аппаратных средств компьютерной системы. В процессе этого происходят нарушения уже установленных правил разграничания доступа процессов и пользователей к ресурсам с информацией. Правилами разграничания доступа называют группу положений, которые регламентируют права доступа процессов или лиц к данным. Наиболее распространены такие нарушения, как:

- противоправное использование привилегий – кража привилегий законных пользователей нарушителем;
- “маскарад” – выполнение тех или иныд действий с данными и системами одним пользователей от имени одного или нескольких лиц;
- перехват паролей – процесс реализуется программами, которые разрабатываются специально для этого.

Процесс передачи и обработки данных техническими средствами компьютерной системы сопутствуется наведением электрических сигналов в линиях связи и электромагнитными излучениями в окрестности. Это явление называется не иначе, как побочные электромагнитные излучения и наводки. Благодаря специальному оборудованию такие сигналы усиливаются, выделяются, принимаются и их можно либо записать на запоминающие устройства, либо просто просмотреть. Электронные излучения могут быть использованы злоумышленниками не столько для получения данных, сколько для её уничтожения или иного вредительства.

Большую угрозу безопасности информации в компьютерной системе представляет несанкционированная модификация алгоритмической, программной и технической структур системы, которая получила название “закладка”. Как правило, “закладки” внедряются в специализированные системы и используются либо для непосредственного вредительского воздействия на КС, либо для обеспечения неконтролируемого входа в систему.

Одним из основных источников угроз безопасности является использование специальных программ, получивших общее название “вредительские программы”. К таким программам относятся:

- “троянские кони” – программы, имеющие вид полезного и безвредного приложения, но на самом деле имеют задачу причинить вред. Пересылка или копирование конфиденциальных данных злоумышленнику, удаление

конфиденциальных данных, выведение из строя программного обеспечения;
- “черви” – программы, запускающиеся при каждой загрузке системы. Обладают способностью проникать в компьютерные системы или сети и создавать там свои копии. К перезагрузке памяти, каналов связи и блокировке системы приводит хаотичное размножение таких программ;
- компьютерные вирусы – программы небольшого размера, проникающие в компьютерную систему и распространяющиеся самостоятельно путём клонирования себя, а при достижении тех или иных условий создают неблагоприятные условия для работы компьютерной системы.

Кроме тех угроз безопасности, что указаны выше, имеется также и угроза утечки информации. Такая угроза с каждым годом становится всё более опасной и значимой проблемой безопасности. Для того, чтобы оперативно справляться с утечками, нужно знать каким образом они происходят.

На долю четырёх основных типов утечек информации приходится огромный процент (84%) инцидентов, при этом около половины от этой доли (40%) случается на одну из самых популярных угроз – кража носителей. 15% приходится на инсайд. К этой категории относятся инциденты, последствием которых стали действия лиц, которые имели легальный доступ к данным. К примеру, сотрудник, не имеющий прав доступа к информационным данным смог обойти систему защиты. Или инсайдер, имеющий полный доступ к данным, вынес её за пределы компании, выложив информацию в общий доступ.

Также 15% всех угроз приходится на хакерские атаки. В эту широкую группу угроз попадают все те утечки, случившиеся благодаря внешнему вторжению. Не самый большой процент хакерских атак можно объяснить тем, что сами незаконные вторжения стали незаметнее.

14% составила веб-утечка. В этот процент пападают те утечки, которые связаны с публикацией закрытых конфиденциальных данных в общедоступных местах, к примеру, в сети Интернет.

9% - это бумажная утечка. Под бумажной утечкой понимается любая утечка, произошедная в результате печати закрытых конфиденциальных сведений и данных на бумажных носителях.

7% составляют другие различные угрозы. В этот процент входят такие инциденты, чью причину установить было крайне трудно или вовсе не удалось, а также утечки, о которых стало известно уже после того, как персональные сведения и данные

были использованы в незаконных целях.

Кроме всего прочего, в данный момент активно развивается фишинг. Фишинг – это технология интернет-пошенничества, заключающаяся в похищении личных, закрытых, конфиденциальных данных, к примеру, банковских счетов, пароли доступа, номера кредитных карт и другой персональной информации. Фишинг (от английского Fishing - рыбалка) – интерпретируется как вылавливание пароля, использует не столько технические недостатки компьютерных систем, сколько наивность и легковерность пользователей сети Интернет.

Информационная безопасность должна сохранять доступность, конфиденциальность, целостность независимо от специфики конкретных видов угроз. Угрозы нарушения доступности, конфиденциальности, целостности стоят на первом месте. Угроза недоступности информации появляется каждый раз, когда из-за сознательных действий злоумышленников или других пользователей закрывается доступ к какому-либо ресурсу компьютерной системы. Нарушение конфиденциальности способно привести к такой ситуации, когда данные могут стать известными тому, кто не имеет полномочий для доступа к таким данным. Нарушение целостности подразумевает под собой любое умышленное изменение данных, которые хранятся в компьютерной системе или которая передаётся из одной системы в другую.

3. Методы и средства защиты информации

3.1 Общая характеристика средств и методов защиты

Сопротивление многочисленным угрозам информационной безопасности подразумевает под собой единое использование всевозможных мероприятий и способов инженерно-технического, криптографического, правового, программно-аппаратного, организационного характера и т.п.

Организационные способы защиты включают в себя множество действий по проверке и подбору персонала, который участвует в эксплуатации и подготовке данных и программ, строгая регулировка функционирования и процесса разработки компьютерных систем.

К средствам защиты и правовым мерам относятся законы, которые действуют в стране, нормативные акты и регулирующие правила обращения с данными и ответственность за их нарушение.

Суть криптографической защиты заключается в том, что происходит приведение информации к неявному виду благодаря специальным аппаратным средствам либо алгоритмам и соответствующим кодовым ключам.

Программно-аппаратные средства защиты применяются непосредственно в компьютерных сетях и компьютерах. Они содержат всевозможные встраиваемые в компьютерные системы электромеханические, электронные устройства. Специальные пакеты программ или же отдельные программы реализуют защитные функции, к примеру, анализ и регистрация активных пользователей, событий, процессов, сопротивление возможным нарушающим стабильную работу, воздействиям на ресурсы, и другие.

Инженерно-технические средства защиты обширны и многообразны. Они включают в себя программные, физико-технические, криптографические, технологические, аппаратные и другие средства. Такие средства обеспечивают такие рубежи защиты, как: контролируемое помещение, здания, территория, отдельные устройства вместе с носителями данных.

3.2 Защита информации от случайных угроз

Одним из самых эффективных способов обеспечения сохранности информации является дублирование информации. Дублирование обеспечивает защиту информации, начиная от случайных угроз и заканчивая преднамеренными воздействиями. Для дублирования данных можно использовать как несъёмные носители информации, так и специальные устройства, которые были разработаны специально для этих целей. Обычные устройства со съёмными носителями также подходят для этой цели. Самым часто встречающимся способом дублирования информации в компьютерных системах представляет собой использование выделенных секторов памяти на рабочем или зеркальном дисках.

Надёжностью называется такое свойство системы, при котором она выполняет поставленные ей задачи в определённых условиях эксплуатации и обслуживания. Надёжность компьютерной системы достигается на этапах эксплуатации, производства и разработки. Своевременное обнаружение и локализация различных неисправностей в работе технических средств компьютерной системы является

важным направлением в обеспечении её надёжности. Современные языки и технологии программирования позволяют значительным образом сократить возможности внесения субъективных ошибок разработчиков.

Свойство компьютерной системы сохранять работоспособность отдельных схем, блоков, устройств называют отказоустойчивостью. Различают 3 основных подхода к созданию отказоустойчивых систем:

- создание адаптивных систем, которые предполагают обеспечение работоспособного состояния компьютерной системы при каком-либо снижении эффективности функционирования в случае отказов элементов;
- помехоустойчивое кодирование информации (рабочую информацию дополняют специальной информацией-кодом, позволяющей обнаружить ошибки и исправлять их);
- простое резервирование (использование схем, блоков, узлов, устройств в качестве резервных).

Минимизация ущерба. Предотвращение стихийных бедствий одними только силами человека пока не представляется возможным, но уменьшить последствия от таких происшествий во многих случаях удаётся. Сведение к минимуму последствий стихийных бедствий и аварий для объектов компьютерной системы может быть достигнуто такими способами:

- обучение персонала противодействию стихийным бедствиям и авариям, способам ликвидации их последствий;
- организация экстренных и срочных оповещений персонала о возможных авариях;
- учет возможных стихийных бедствий и аварий при эксплуатации и разработки компьютерных систем;
- разумный выбор места расположение объекта вдали от тех мест, где возможны стихийные бедствия;

Оптимизация. Сокращение численности ошибок персонала и пользователей, сведение к минимуму последствий таких ошибок является одним из основных направлений защиты информации. Для достижения этих целей нужно совершенствование и анализ процессов взаимодействия человека и компьютерной системы, обучение и воспитание персонала и пользователей, научная организация труда.

Блокировка ошибочных операций. Ошибочные операции в работе компьютерной системы могут быть вызваны не только случайными отказами программных или технических средств, но и ошибками обслуживающего персонала и пользователей. Для того, чтобы заблокировать ошибочные действия, используют аппаратно-программные и технические средства, к примеру, средства блокировки записи на магнитные диски, предохранители и блокировочные тумблеры.

3.3 Защита компьютерной системы от несанкционированного вмешательства

Для блокирования (парирования) случайных угроз безопасности в КС должен быть решен комплекс задач, что показано в приложении 2.

Внедрение так называемых средств AAA (ЗА) (администрирование, авторизация, аутентификация) является основным способом защиты от злоумышленников.

Авторизация – это процедура, по которой пользователь во время входа в систему распознаётся и получает доступ, который разрешён системным администратором, к вычислительным системам и ресурсам.

Авторизация происходит путём выполнения программой аутентификации и идентификации.

Аутентификация – это проверка подлинности. То есть того, что предоставленный идентификатор, в самом деле, принадлежит субъекту доступа. Выполняется на основе сравнения пароля и имени пользователя. После удачной аутентификации субъекту открывается доступ к данным и ресурсам системы в рамках полномочий, что разрешены этому субъекту.

Идентификация – это предоставление идентификатора, который может представлять собой число, слово или несекретное имя, для регистрации пользователя в компьютерной системе. Субъект вводит имя пользователя и представленный идентификатор сравнивается со списком идентификаторов. Тот пользователь, чей идентификатор зарегистрирован в системе, будет расцениваться как легальный.

Методы авторизации, которые основаны на использовании паролей применяются чаще остальных. Установить пароль можно как на отдельные действия в сети или на компьютере, так и на запуск отдельно взятых программ. Также вместо паролей

для подтверждения подлинности могут быть использованы смарт-карты или пластиковые карточки.

Регистрацией действий пользователя в сети, а также его попытки доступа к данным называют администрированием. Для контроля за соблюдением установленных прав доступа, для своевременного пресечения несанкционированных действий необходимо обеспечить регулярную выдачу, фиксацию и сбор по запросам сведений обо всех попытках доступа к защищаемым ресурсам компьютерной системы. Ведение специальных регистрационных журналов, которые представляют собой файлы на внешних носителях данных, являются основной формой регистрации.

Зачастую утечка данных происходит из-за несанкционированного копирования данных. Такая угроза может быть блокирована:

- методами, которые препятствуют использованию данных или затрудняют чтение и использование полученных копированием данных и программ. Одним из самых эффективным средством защиты в этом отношении представляет собой хранение данных в преобразованном виде с помощью криптографических методов. Использование блока контроля среды размещения программ является другим методом противодействия несанкционированному выполнению скопированных данных и программ. Этот метод создаётся при установке программы и включает в себя характеристики среды, где размещена программа, а также средства сравнения этих характеристик. В роли характеристик могут быть использованы характеристики носителя информации или ЭВМ;
- методами, которые затрудняют считывание скопированных данных. Такие методы в процессе записи информации на соответствующие накопители создают особенности, не позволяющие считывать полученную копию на других накопителях, которые не входят в состав защищаемой компьютерной системы. Проще говоря, такие методы созданы для обеспечения совместимости накопителей только внутри отдельно взятой компьютерной системы.

Для защиты компьютерных систем от всевозможных вредоносных программ разработаны специальные антивирусные средства.

Антивирусной программой называют часть программного обеспечения, устанавливаемой на компьютер для поиска вирусов на дисках и во входящих файлах для последующего удаления или лечения при обнаружении.

Программа обнаруживает вирусы и предлагает вылечить файлы, либо при невозможности лечения удалить. Существует несколько разновидностей антивирусных программ:

- блокировщики – отслеживают события и перехватывают подозрительные действия, запрещая действия или запрашивая для этого разрешение пользователя;
- иммунизаторы – обнаруживают подозрительные действия работы компьютера, которые характерны для вируса на ранней стадии, после чего посылают пользователю предупреждающее сообщение; предотвращают заражение файлов;
- мониторы – проверяют оперативную память при загрузке операционной системы. Автоматически проверяют файлы в момент открытия и закрытия, не допуская открытия и записи файла, который заражён вирусом. Блокирует вирусы;
- доктора – кроме того, что находят заражённые вирусами файлы, ещё и лечат их. Иными словами удаляют из файла тело программы-вируса, при этом возвращая файлу его исходное состояние;
- ревизоры – запоминают исходное состояние каталогов, программ до заражения их вирусами и периодически сравнивают текущее состояние системы с записанным ранее;
- программы-фаги или сканеры – это программы поиска в загрузочных секторах дисков, памяти, файлах сигнатур вирусов, проверяют и лечат файлы.

3.4 Криптографические методы защиты информации и межсетевые экраны

Закрытие информации методами криптографического преобразования является одним из эффективных средств противодействия различным угрозам информационной безопасности. Благодаря такому преобразованию, информация, которая защищена, становится недоступной для использования и ознакомления тем лицам, которые не имеют на это полномочий. По методу воздействия на исходные данные криптографические методы разделены на следующие виды:

кодирование – замена смысловых конструкций исходных данных кодами. В качестве кодом можно использовать сочетания цифр и букв. При кодировании и обратном преобразовании используются специальные словари и таблицы, которые хранятся в секрете. Для защиты данных от искажений в канала связи зачастую

используют кодирование.

Стеганография – метод зашиты компьютерных данных, которые передаются по каналам телекоммуникации, путём скрытия сообщения среди открытого звука, изображения или текста в файле-контейнере. Данный метод позволяет скрыть не только смысл передаваемых и хранящихся данных, но и сам факт передачи или хранения закрытых данных. Скрытый файл может быть зашифрован. В случае случайного обнаружения скрытого файла, зашифрованные данные будут восприняты как сбой в работе системы.

Шифрование – процесс маскировки информации или сообщений с целью ограничения доступа к содержанию другим лицам. Такой процесс заключается в проведении обратимых комбинаторных, логических, математических и других преобразований исходных данных, благодаря которым зашифрованные данные представляют собой несвязанный между собой набор цифр, букв, двоичных кодов и других символов. Для шифрования используется ключ и алгоритм преобразования.

Сокращение объёма данных является целью сжатия этих данных. Однако, сжатые данные не могут быть использованы или прочитаны, пока не будут преобразованы обратно. Учитывая то, что средства сжатия и обратного преобразования доступны широкому кругу пользователей, такие методы сложно рассматривать как надёжные средства криптографического преобразования данных. Поэтому сжатые файлы подвергаются последующему шифрованию.

Рассечение-разнесение заключается в том, что массив данных, которые защищается, делится на множество элементов, каждый из которых по отдельности не позволит раскрыть содержание защищённых данных. Выделенные таким образом элементы информации располагаются на различных носителях или разносятся по разным зонам запоминающих устройств.

Строкой данных, зависящая от некоего секретного параметра, известного лишь подписывающему лицу, и от содержания подписываемой информации, которая представлена в цифровом виде является электронная цифровая подпись. Такая подпись используется для подтверждения авторства и целостности информации. Изменить документ без нарушения целостности подписи нельзя.

Специальное аппаратно-программное средство или программное обеспечение, которое носит название “межсетевой экран” или “firewall” используется для блокировки угроз, которые исходят из общедоступных систем. Межсетевой экран позволяет разделить общую сеть на две или более части и реализовать набор

правил, которые определяют условия прохождения пакетов с информацией из одной части общедоступной сети в другую. Зачастую сетевая защита может полностью блокировать трафик, который идёт извне, но полностью разрешить внутренним пользователям свободно контактировать с внешним миром. Как правило, межсетевой экран защищает внутреннюю сеть предприятия от вторжения или атак из глобальной сети интернет. Межсетевой экран может выполнять четыре основные функции:

- регистрация событий в специально отведённых для этого журналах. Анализ записей даёт возможность зафиксировать попытки нарушения установленных правил обмена данными в сети и выявить злоумышленника;
- трансляция адресов предназначена для маскировки истинных внутренних адресов от внешних абонентов;
- использование экранирующих агентов, являющихся программами-посредниками, которые обеспечивают связь между объектом доступа и субъектом, а затем пересылают данных, осуществляя регистрацию и контроль;
- фильтрацию информации на различных уровнях.

Заключение

В этой работе были охарактеризованы основные виды угроз информационной безопасности, а также были рассмотрены имеющиеся на данный момент средства и методы защиты информации.

Обусловленность уязвимости информации в компьютерных системах заключается в её территориальной рассредоточенности, большой концентрацией вычислительных ресурсов, одновременным доступом к ресурсам компьютерных сетей многочисленных пользователей, долговременным хранением больших объёмов данных. Ежедневно на свет появляются новые угрозы, такие как: несанкционированные вмешательства или сетевые атаки, из-за этого, сколько бы времени не проходило, а острота проблемы информационной безопасности не уменьшается, а напротив, становится всё актуальней.

В результате удачных атак против информационной безопасности может быть нанесён серьёзный ущерб жизненно важным интересам страны в оборонной, экономической, политической и других сферах деятельности. Может быть причинен социально-экономический ущерб отдельным лицам или обществу. Исходя

из этого, можно сделать вывод, что информационная безопасность – это комплекс мер, среди которых трудно выделить важным что-то одно.

Сопротивление многочисленным угрозам информационной безопасности подразумевает под собой единое использование всевозможных мероприятий и способов инженерно-технического, криптографического, правового, программно-аппаратного, организационного характера и т.п.

Организационные способы защиты включают в себя множество действий по проверке и подбору персонала, который участвует в эксплуатации и подготовке данных и программ, строгая регулировка функционирования и процесса разработки компьютерных систем.

Список использованной литературы

1. Агальцов В.П., Титов В.М. Информатика для экономистов: Учебник. – М: ИД “ФОРУМ”: ИНФРА-М, 2006. – 448 с.
2. Гаврилов М.В. Информатика и информационные технологии: Учебник. – М: Гардарики, 2006. – 655 с.
3. Домарев В.В. Безопасность информационных технологий. – К: ООО “ТИД “ДС”, 2004. – 992 с.
4. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М: Логос; ПБОЮЛ, 2001. – 264 с.
5. В.П. Косарева и Л.В. Еремина Компьютерные системы и сети: Учебное пособие. М: Финансы и статистика, 2001. – 464 с.
6. Коуров Л.В. Информационные технологии. – Мн.: Амалфея, 2000. – 192 с.
7. Семененко В.А. Информационная безопасность: Учебное пособие. – М: МГИУ, 2005. – 215 с.
8. Шальгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М: ДМК Пресс, 2008. – 544 с.

Приложения