Содержание:

Введение

Проблема обеспечения требуемого уровня защиты данных в нынешнее время охватывает целое множество параметров, к примеру, физическую защиту системных программ и информации, защиту от предотвращения несанкционированного доступа к информации, передаваемым по каналам связи и находящимся непосредственно на накопителях, являющегося результатом работы посторонних лиц и специальных программных продуктов – вирусов.

Если принимать во внимание тот факт, что ядром информационной системы (ИС) является система управления базами данных СУБД, то обеспечение требуемого уровня информационной безопасности приобретает определяющее значение при непосредственном выборе конкретных инструментов обеспечения безопасности в целом организации.

Данные, которые используются в компьютерной форме сосредотачиваются в небольшом и физически локальном объеме (к примеру, на флэш-карте) огромные массивы структурированных данных, несанкционированный доступ к которым или их разрушение могут приводить к ущербу и катастрофическим последствиям.

Возможность копирования за короткое время, модификации или удаления массивов данных, что находятся в компьютерной форме, или удаленно расположенных, провоцирует злоумышленников дополнительно на несанкционированный доступ к хранимой информации, выполнение ее модификации или разрушение.

Стоит отметить, что теоретическая проработка вопросов по обеспечению безопасности информации, а также их практическая реализация отставали долгое время от уровня развития все совокупности программной индустрии СУБД, при чем в коммерческих продуктах такие методы обеспечения безопасности данных начали появляться только в 90-х годах XX столетия.

Первые исследования практики и теории обеспечения безопасности информации в компьютерных системах обуславливались, прежде всего, потребностями оборонной сферы, где постоянно существующая проблема компьютерной безопасности стоит

особенно остро.

Начало данным процессам было положено работами по защите компьютерной информации, которые проведены в конце 1970-х годов национальным центром безопасности Министерства обороны США.

Главным результатом этих исследований было издание Министерством обороны документа под наименованием «Критерии оценки компьютерных систем».

Стоит отметить, что он была одним с самых первых документов, который регламентировал инструменты по обеспечению требуемого уровня защиты данных.

Актуальностью работы является рассмотрение виды и состава угроз информационной безопасности, так как данная проблема является одной с самых основоположных в настоящее время.

Цель курсовой работы – рассмотреть основные типы и состав информационной безопасности, а также рассмотреть инструменты для обеспечение защиты данных.

В соответствии с целью поставлены такие задачи:

– рассмотреть основные понятия по теории информационной безопасности;

– описать угрозы ИБ в зависимости от источников и мотивации;

– дать характеристику типам воздействий, которые представляют угрозу в вычислительных системах;

– рассмотреть организационно-правовые и технические средства защиты данных;

– описать криптографические и аппаратно-программные средства защиты данных.

Объект работы – теория информационной безопасности;

Предмет работы – классификация угроз информационной безопасности.

Курсовая работа состоит с введения, основной части, заключения и списка использованных источников.

1.Основные понятия об информационной безопасности

1.1 Определение информационной безопасности

Примечательная особенность нынешнего периода – это переход от индустриального социума к информационному, в котором информация далее становится важным ресурсом, чем энергические или материальные ресурсы. Ресурсами называют элементы из экономического потенциала, которыми общество располагает и которое могут быть использованы при необходимости для достижения конкретных целей хозяйственной деятельности.

Также давно стали общеупотребительными и привычными такие категории, как финансовые, трудовые, материальные, природные ресурсы, что вовлекаются в хозяйственные обороты, и их назначение будет понятно каждому. [5]

После появления понятия "информационные ресурсы" – оно узаконено, но пока еще осознано недостаточно.

Информационные ресурсы – это отдельные документы или отдельные массивы документов для информационных систем (библиотеках, архивах, банках данных, фондах, других информационных системах). [10]

Информационные ресурсы также являются собственностью, и находятся в ведении органов и организаций, также подлежат учету, защите, поскольку информацию можно применять не только для услуг и товаров, но и превращать ее в наличность, кому-нибудь продав, или, что хуже, уничтожить. Информация для производителя также представляет значительную ценность, поскольку нередко получение (или создание) такой информации – это весьма трудоемкий дорогостоящий процесс.[15]

Информационная безопасность — состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере.

Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации.

Моделирование процессов нарушения такой безопасности информации осуществлять целесообразно на базе рассмотрения логической цепочки типа: «угроза – источник угрозы – способ реализации – уязвимость – результат» (рисунок 1).

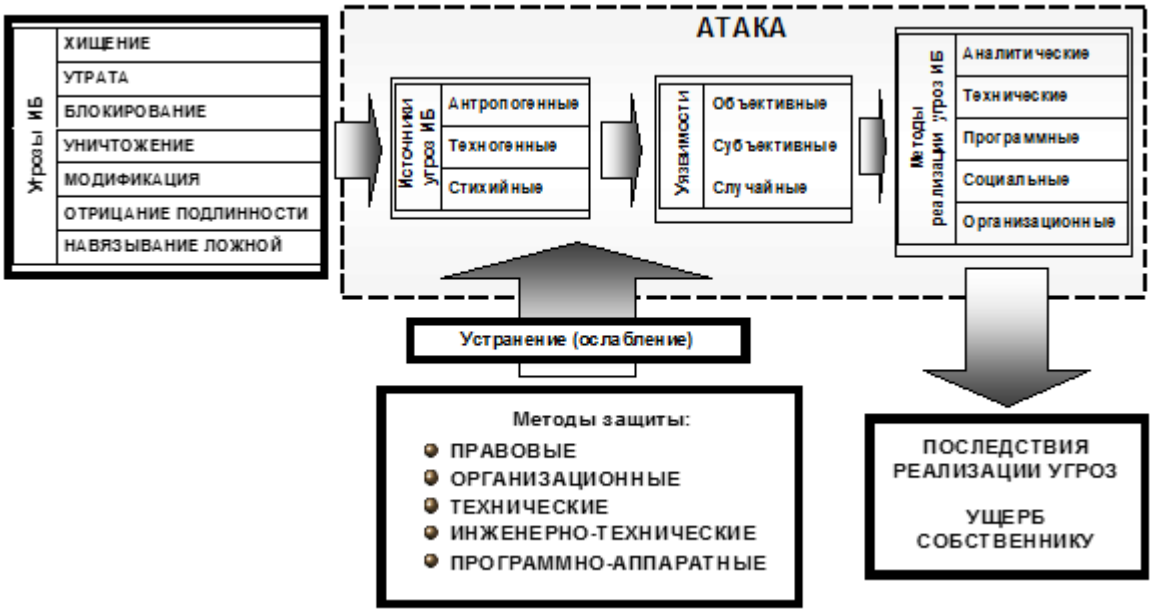

Рис.1. Модель реализации угроз для информационной безопасности (ИБ)

В ходе анализа надо убедиться, что все источники возможных угроз идентифицированы, также все возможные уязвимости идентифицированы, сопоставлены со всеми идентифицированными источниками угроз, а всем идентифицированным уязвимостям (факторам) и источникам угроз сопоставлены методы реализации.[20]

При этом важно использовать возможность, при необходимости, вовсе не меняя самого инструментария, вводить новые типы источников угроз, уязвимостей, методов реализации, которые станут известными в результате развития учений в этой области [4].

Как видно, анализ для негативных последствий реализации разных угроз предполагает обязательную и безоговорочную идентификацию (к примеру, присвоение уникального кода) для всех возможных источников угроз, разных уязвимостей, способствующих проявлению их и методов реализации.

Сам подход для анализа и оценке состояния по безопасности информации основывается также на вычислении некоторых весовых коэффициентов опасности при источниках угроз и уязвимостей, а также и сравнения этих коэффициентов с заданным заранее критерием и последовательном исключении полного перечня возможных натуральных источников угроз до минимально актуального при конкретном объекте.[12]

Рис.2. Алгоритм проведения анализа и оценки

Результаты проведения анализа и оценки (рисунок 2) могут быть использованы для выбора адекватных оптимальных методов при парирования угроз, а также при выполнении аудита реального состояния ИБ объекта для разных целей его страхования.

1.2. Понятие нарушителя безопасности

Модель вероятного нарушителя для безопасности ИС необходима в основном для систематизации информации по типах и возможностях разных субъектов, целях выполнения несанкционированных воздействий, а также выработки адекватных технических и организационных мер противодействия.

При разработке модели для нарушителя ИС учитываются факторы:

– предположения о категориях разного рода лиц, к которым принадлежит нарушитель; [1]

– типы нарушителя;

– предположения мотивов действий нарушителя;

– предположения о квалификации нарушителей и его аппаратной оснащенности;

– ограничения и предположения по характеру возможных действий нарушителей;

– непосредственный характер информационных угроз.

Стоит отметить, что по наличию права разового или постоянного доступа нарушители подразделяются на 2 типа:

– нарушители, что не имеют доступа к ИС, но реализующие угрозы с внешних сетей связи для общего пользования;

– нарушители, имеющие уровень доступ к ИС, при этом включая пользователей, что реализуют угрозы непосредственно в ПО, внутренние нарушители.

1.3.Правовые основы моделей нарушителя безопасности правовых данных

Согласно [10] внешний нарушитель имеет такие возможности:

– выполнять несанкционированный доступ к разного рода каналам связи, что выходят за пределы разных служебных помещений;

– выполнять несанкционированный доступ через так называемые автоматизированные рабочие места, что подключены к сетям связи для общего пользования и сетям международного обмена данными;

– осуществлять несанкционированный доступ непосредственно к информации с применением специальных программных воздействий при помощи вредоносных программ, программных вирусов, алгоритмических и программных закладок;

– выполнять несанкционированный доступ через компоненты информационной инфраструктуры ИС, что в процессе жизненного цикла (сопровождения, ремонта, модернизации, утилизации) оказываются за границами контролируемой зоны;

– реализовать несанкционированный доступ с помощью ИС взаимодействующих ведомств и учреждений.

Внешний тип нарушителя:[7]

– криминальные структуры;

– разведывательные службы государств;

– представители конкурирующих организаций или лица, что действуют по их заданию;

– так называемые недобросовестные партнеры;

– разные клиенты (граждане, представители организаций);

– посетители (приглашенные по некоторому поводу);

– представители организаций, что взаимодействующих по вопросам уровня обеспечения жизнедеятельности организации;

– лица, умышленно или случайно нарушившие пропускной режим.

Внутренний тип нарушителя:

– пользователи ИС;

– администраторы ИС;

– персонал, обслуживающий технические средства (инженеры, техники);

– сотрудники отделов;

– технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения);

– сотрудники службы безопасности; руководители различных уровней должностной иерархии.

В результате рассмотрения первой главы курсовой работы описаны основные понятия теории информационной безопасности, дана характеристика понятию нарушителей ИБ и их правовые основы.

2. Угрозы безопасности информации, их классификация

2.1. Угрозы в зависимости от мотивации

Под угрозой безопасности для информации понимается всевозможное событие, явление или процесс, которое может приводить к уничтожению, утрате уровня целостности, конфиденциальности и доступности информации. Полностью все множество потенциальных угроз для безопасности информации может быть разделено на несколько классов.

Угрозы, которые никак не связаны с полностью преднамеренными действиями злоумышленников, а также реализуются в полностью случайные моменты времени, называют случайными (непреднамеренными).[3]

К таким случайным угрозам можно отнести:

– стихийные бедствия;

– аварии;

– отказы технических средств;

– сбои;

– ошибки при разработке КС и другие.

Реализация угроз данного класса приводит непосредственно к наибольшим потерям данных (до 85 % от всего ущерба, наносимого ресурсам КС всеми угрозами).

При этом может выполняться уничтожение, а также нарушение доступности и целостности информации.

Реже нарушается уровень конфиденциальность данных, однако при этом могут создаваться предпосылки для воздействия злоумышленника на информацию.

Согласно статистическим данным только после ошибок пользователей и обслуживающих сотрудников происходит до 60% случаев нарушения уровня безопасности информации.

Также, следует отметить, что механизмы реализации случайных угроз изучены достаточно хорошо, а также накоплен значительный опыт в противодействии этим угрозам.

Также все современная технология разработки программных и технических средств, эффективная система их эксплуатации, включающая обязательное резервирование данных, позволяют значительно снижать потери от реализации всех угроз данного класса.

Угрозы, что связаны с злоумышленными действиями персонала, а эти действия уже носят не просто непреднамеренный характер, а являются преднамеренными.

К преднамеренным угрозам часто относятся традиционный или же универсальный шпионаж, диверсии, выполнение несанкционированного доступа к информации, наводки и электромагнитные излучения, несанкционированная модификация структур, а также вредительские программы.

В качестве источников для нежелательного воздействия на разного рода информационные ресурсы актуальны по-прежнему средства и методы шпионажа и диверсий.

Стоит отметить, что к методам диверсий и шпионажа относятся:[6]

– визуальное наблюдение;

– подслушивание;

– хищение документов и носителей информации;

– хищение атрибутов систем защиты и программ;

– подкуп и шантаж персонала;

– сбор и анализ машинных носителей информации, а также поджоги, взрывы;

– нападения диверсионных групп.

Также, стоит отметить, что основные непреднамеренные угрозы для ЛВС такие:

– неумышленные действия, что приводят полному отказу ЛВС или разрушению ресурсов системы (порча оборудования, удаление, искажение файлов);[2]

– неправомерное отключение аппаратной техники и изменение графика функционирования программ;

– порча носителей данных;

– запуск сторонних программ для потери работоспособности ЛВС или осуществляющих в ней критические изменения;

– нелегальное внедрение нелицензионных программ;

– заражение вирусами и другие.

Следует заметить, что при достижении поставленных целей чаще всего злоумышленники используют сразу совокупность с выше перечисленных методов.

2.2. Угрозы по источникам

Источники угроз – условия и факторы, что таят в себе угрозы, а при определенных условиях в различной совокупности обнаруживают некоторые враждебные намерения, деструктивную природу и вредоносные свойства. Источники угроз можно различить по таким факторам:

– техногенному;

– естественно-природному;

– социальному.

Антропогенными источниками угроз защиты ЛВС выступают субъекты, которые выполняют действия, что квалифицированы как умышленные или случайные преступления (рисунок 3).

Рис.3. Антропогенные источники угроз

Только в данном случае можно вести речь о причинении ущерба. Такие группы наиболее обширны и представляют наибольший интерес для реорганизации защиты, так как действия таких субъектов можно всегда прогнозировать.

В качестве антропогенных источников часто рассматривают субъекты, что имеют доступ (как несанкционированный, так и санкционированный) к выполнению работы с штатными средствами для защищаемого объекта безопасности.

Вторая группа в себе содержит такие источники, которые определяются так называемой технократической деятельностью людей, а также и развитием цивилизации.

В результате их последствия, вызванные такой деятельностью, вышли из-под контроля человека уже давно, они существуют в данный момент сами по себе. [4]

Указанные источники угроз намного сложнее спрогнозировать, а также они напрямую зависят от свойств аппаратного сетевого обеспечения (рисунок 4).

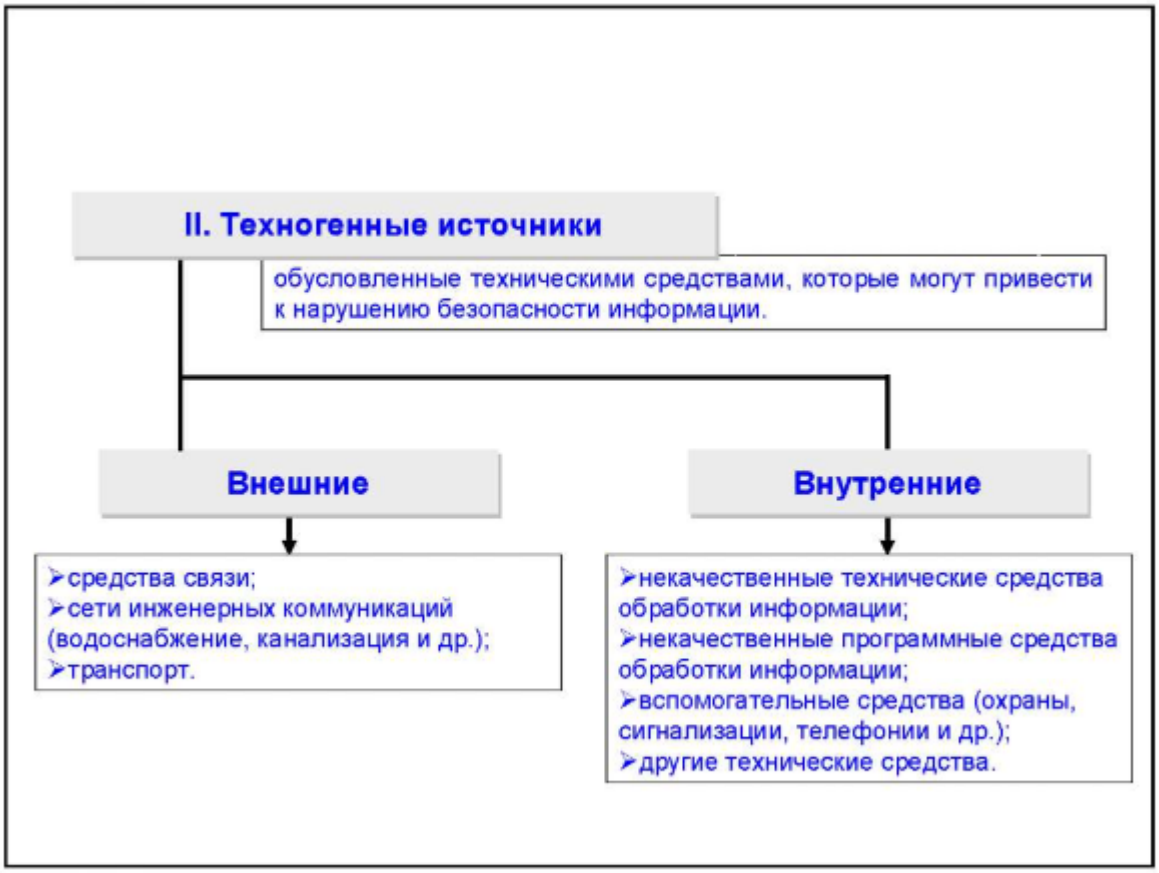

Рис.4. Технократические источники угроз

Этот класс источников особенно актуален в данное время, поскольку в сложившихся сложных условиях все такие эксперты ожидают значительного увеличения численности техногенных катастроф, которые будут вызваны физическим устареванием аппаратного сетевого оборудования в ОВС организаций.

Третья группа описываемых источников угроз в себе объединяет практически все обстоятельства, которые составляют некую непреодолимую силу, а также обстоятельства, носящие объективный характер и распространяются полностью на все средства программного или аппаратного обеспечения некоторой местности (рисунок 5).

Рис.5. Стихийные источники

В законодательстве РФ к данной категории относят стихийные бедствия, а также иные обстоятельства, что практически невозможно предусматривать, предотвратить при нынешнем уровне знания и возможностей.

Стихийные источники всегда являются внешними непосредственно к защищаемому объекту, а также понимаются под ними природные катаклизмы и катастрофы.

2.3. Типы воздействий, которые представляют угрозу в вычислительных сетях

Все удаленные атаки на защиту ЛВС можно классифицировать по таким признакам.

В зависимости от характера и типа воздействия на работу ЛВС удаленные атаки могут разделяться на такие категории:

– пассивные;

– активные.

Пассивное воздействие для распределенной вычислительной системы не связано с влиянием непосредственно на работу системы, хотя нарушает ее политику безопасности.

К примеру, прослушивание канала связи, который присутствует в ЛВС. [5]

При этом, активным воздействием на вычислительную распределенную систему называют воздействие, которые оказывают непосредственное влияние на функционирование системы (нарушение работоспособности, изменение конфигурации и прочее) и нарушающее в ней принятую политику безопасности.

В современное время практически все классы удаленных атак считаются активными воздействиями по таким причинам.

– в зависимости от конечной цели осуществления атаки они могут распределяться на угрозы, что связаны с нарушением конфиденциальности, целостности информации и отказа в его обслуживании.

Самая основная цель для практически любой атаки – это получить несанкционированный доступ к нужным данным.

Также в теории защиты информации существуют 2 принципиальные возможности для выполнения доступа к информации – это:

– перехват;

– искажение.

При этом возможность перехвата информации под собой подразумевает получение доступа к ней, но невозможность в ее модификации.

Классическим примером перехвата данных может служить прослушивание телефонной линии.

Возможность искажения данных значит, что достигнут или полный контроль над потоком информации между объектами ЛВС, или возможность передачи данных от имени иного объекта.

Стоит отметить, что при нарушении работоспособности ЛВС основная цель для атакующего – добиться, чтоб сетевая ОС на атакуемом объекте полностью вышла из строя, а для всех остальных субъектов системы доступ к всем ресурсам был бы невозможен.[2]

Также возможны и иные классификации удаленных атак, к примеру: в зависимости от условий воздействия, от наличия обратной связи, от места расположения субъекта.

3. Инструменты обеспечения требуемого уровня защиты данных

3.1. Организационно-правовые и технические средства

Вопросы защиты информационных информации в ЛВС самым тесным образом связываются не только с решением технических проблем, но и с разными вопросами правового регулирования в процессе передачи данных и информатизации.

Необходимость организационно-правового инструментария для защиты информации вытекает непосредственно из факта признания информации товаром, продукта общественного производства, а также установления в порядке законов права собственности на нее.

Такая постановка приобретает смысл и характер непосредственно в условиях демократизации для общества, формирования экономики, включения РФ в мировое сообщество.

Организационно-правовое обеспечение читается многоаспектным понятием, которое включает законы, решения, а также нормативы и правила. Стоит отметить, что применительно к защите данных, обрабатываемой в АИС, оно имеет целый ряд принципиальных особенностей, которые обусловлены следующими обстоятельствами:

- представлением данных в непривычной для человека форме;

- использованием разного рода носителей информации, на которых просмотр не является очевидным;[9]
- возможностью многократного использования информации без оставления следов;
- легкостью корректировки любых элементов данных без оставления исправления;
- наличием большого количества нетрадиционных факторов, оказывающих влияние на безопасность информации.

Из практических соображений становится ясно, что так называемая организационно-правовая база защиты данных должна включать в себя:

- определение подразделений, ответственных за организацию безопасности информации;
- руководящие и методические, а также правовые материалы по защите информации;
- разного рода меры ответственности за непосредственное нарушение правил безопасности;
- порядок разрешения конфликтных ситуаций по вопросу защиты информации в ЛВС.

Таким образом, полностью вся совокупность вопросов, что возникают при решении проблем в направлении организационно-правового обеспечения, представляется в виде схемы (рисунок 6).[13]

Группа технических средств для защиты информации в себе совмещает как аппаратные, так и программные средства. Главные из них такие:

– резервное копирование, а также удаленное хранение самых важных массивов информации в компьютерной системе;

– дублирование, а также резервирование подсистем сетей, что имеют значение в секторе сохранности информации;

– создание возможности для перераспределения ресурсов сети в случаях непосредственного нарушения работоспособности элементов;

– обеспечение возможности применять резервные системы для обеспечения электропитания;

– обеспечение безопасности информации и ЛВС от пожара или наводнений;

– установка качественного ПО, которое обеспечивает защиту ЛВС от несанкционированного доступа.[7]

Рис.6. Организационно-правовое обеспечение

Заметим, что в комплекс технических мер также входят и меры для обеспечения физической недоступности объектов ЛВС, к примеру, такие практические методы, как оборудование помещения сигнализацией или видеокамерами.

3.2. Криптографические средства

Криптография – это наука о защите данные от прочтения их посторонними лицами.

Такая защита достигается методами шифрования, то есть, преобразованием, что делают защищенные исходные данные труднораскрываемыми по начальным данным без знания ключевой информации, что называется ключом.

Под ключом понимают легко изменяемую часть криптосистемы, что хранится в тайне, а также определяется, какое именно шифрующие преобразование с возможных выполняется в этом случае.

Криптосистема – это семейство выбираемых при использования ключа обратных преобразований, что преобразуют защищаемый текст в шифрограмму.

Методы шифрования должны обладать минимум 2-я свойствами:

– получатель сможет выполнить дешифрование и расшифровать данные;

– криптоаналитик противника, что перехватил сообщение, не сможет его восстановить без таких затрат средств и времени, которые сделают данную работу нецелесообразной.[1]

Заметим, то в современной криптографии есть два типа алгоритмов, а именно:

– классический, что основан на применении секретных ключей;

– новые алгоритмы, которые используются как открытые или закрытые ключи.

Криптографические средства для защиты информации, применяют все возможности для шифрования сообщений, с помощью ключей, а также и путем применения генераторов псевдослучайных чисел.

Заметим, что последний метод такой защиты легко реализуется, а также обеспечивает высокую скорость как шифрования, так и дешифрования, но не всегда он стоек к дешифровке так как и неприменим для больших информационных систем.

Однако самыми перспективными средствами для защиты конфиденциальной информации считают асимметричные криптосистемы с открытым ключом.

Основная суть такой системы в том, что все ключи дешифровки и шифрования не совпадают.

С таком случае, криптографические средства для защиты информации в рассматриваемых криптосистемах заключены в том, что при шифровании

используется только открытый ключ, что известен всем, а при дешифровки применяется секретный ключ, что известен только конечному получателю. Этот способ защиты очень эффективен для передачи информации и не часто применим при её хранении.

Надежная криптографическая система соответствует ряду требований [10]:

– зашифровывание, дешифровка должны являться понятными и прозрачными.

– дешифровка конфиденциальных данных третьими лицами должна быть затруднена.

– содержание информации сказываться не должно на эффективности алгоритмов.[8]

Криптографические средства для защиты информации, что базируются на применении кодов и ключей, преследуют цели эффективного уровня защиты данных, а также снижения трудоемкости выполнения работы с информацией, непосредственного обеспечения быстрой обработки, экономии объемов памяти компьютера, а также формализации описания информации, основываясь на систематизации их и классификации.

В настоящее время в РФ действуют 3 государственных стандарта для криптографической защиты информации, что определяют базовые криптографические алгоритмы, а именно:

– симметричное шифрование;

– хэш-функция;

– электронная цифровая подпись.

3.3. Аппаратно-программные средства защиты информации

Первые операционные системы для ПК не имели каких-то собственных средств защиты, а это породило проблему создания инструментария для данных.

Актуальность этой проблемы не уменьшилась практически с появлением мощных ОС, что имели развитые подсистемы защиты, к примеру, ОС Windows NT.[9]

Это обусловлено также тем, что множество систем не способны защищать данные, находящиеся полностью за ее пределами, к примеру, при использовании информационного сетевого обмена.

Аппаратно-программные средства защиты данных, обеспечивающие повышенный уровень безопасности можно разбить на 5 основных групп (рисунок 7).

Рис.7. Аппаратно-программные средства защиты данных

Первую группу образуют специальные системы аутентификации и идентификации пользователей.

Эти системы применяются только для ограничения доступа незаконных пользователей непосредственно к ресурсам ЛВС. Общий алгоритм работы систем заключается в том, чтоб получить от пользователя всю информацию, которая удостоверяет его личность, а также проверить ее подлинность, затем предоставить пользователю возможность работы с ней.

При построении подобных систем часто возникает проблема в выборе информации, на базе которой осуществляются все процедуры идентификации пользователя.

При этом можно выделить такие типы:

– секретная информация, что обладает пользователь (персональный идентификатор, пароль, секретный ключ);

– физиологические параметры человека (рисунок радужной оболочки, отпечатки пальцев) или особенности поведения субъекта.[6]

Системы идентификации, что основаны на первом виде информации, являются традиционными.

Все системы идентификации, что применяют второй тип данных, называются биометрическими.

Также следует отметить в последнее время наметившуюся тенденцию развития биометрических систем для идентификации пользователей.

Вторую группу средств, что обеспечивают повышенный уровень защиты, содержат системы шифрования так называемых дисковых данных. Главная задача, решаемая данными системами, состоит непосредственно в защите данных от несанкционированного использования, расположенных на носителях.

Обеспечение конфиденциальности информации, располагаемых на разных магнитных носителях, выполняется путем их шифрования с применением симметричных алгоритмов шифрования.

Главным классификационным признаком комплексов шифрования служит степень их встраивания в ЛВС.

Работа разных прикладных программ с накопителями состоит из 2-х этапов:

– логического;

– физического.

Логический этап используется при соответствии уровню взаимодействия определенной прикладной программы с ОС (например, вызов функций чтения данных).

Физический этап соответствует степени взаимодействия операционной системы, а также аппаратуры.

В качестве разного рода объектов данного уровня выступают различные структуры физической организации информации – сектора диска. [3]

После этого, системы шифрования информации могут осуществлять различные криптографические преобразования информации на уровне файлов и на уровне физических дисков.

К третьей категории средств, обеспечивающих увеличенный уровень защиты, относят системы шифрования информации, передаваемой по компьютерным сетям.

При этом различают два главных способа шифрования:

– канальное;

– оконечное

В случае канального метода защищается вся по каналу связи передаваемая информация, включая также служебную информацию. Соответствующие процедуры шифрования также могут реализоваться с помощью протоколов канального уровня эталонной модели взаимодействия систем OSI.

Данный способ шифрования обладает таким достоинством – встраивание разных процедур шифрования на некоторый уровень позволяет применять аппаратные средства, способствующие повышению производительности всей системы.

Однако, в данного подхода есть существенные недостатки:

– шифрованию на указанном уровне подлежит практически вся информация; это осложняет механизмы маршрутизации сетевых пакетов данных и требует расшифрования информации в устройствах для промежуточной коммутации;

– шифрование служебных данных, неизбежное на этом уровне, может также привести к непосредственному появлению статистических закономерностей для шифрованных данных.

Оконечное шифрование позволяет обеспечивать конфиденциальность данных, что передаются между двумя объектами (абонентами). [4]

Оно реализуется при использовании протокола прикладного, а также представительного уровня модели OSI.

Четвертую группу средств для защиты составляют так называемые системы для аутентификации электронных данных.

С точки зрения обмена электронных данных по сетям связи часто возникает проблема аутентификации авторов документа, а также самого документа, то есть, установление подлинности автора, а также проверка отсутствия изменений в документе.

При аутентификации электронных данных часто применяют код аутентификации (имитовставку), а также электронную цифровую подпись.

Аналогичные возможности предоставляет и отечественный стандарт для организации симметричного шифрования информации ГОСТ 28147-89.

Этот алгоритм использует режим выработки имитовставки, что обеспечивает имитозащиту, то есть, защиту системы шифрованной от навязывания ложной информации.

Имитовставка вырабатывается с открытых данных при использовании специального преобразования шифрования при применении секретного ключа, а также передается по каналам связи в конце данных.

Пятую группу средств, что обеспечивают повышенный уровень защиты, составляют средства управления базовой информацией. Под ключевыми данными понимается совокупность практически всех используемых в системе или сети ключей криптографических алгоритмов.

Безопасность любого алгоритма определяется применяемыми криптографическими ключами.

Стоит отметить, что в случае ненадежного управления такими ключами злоумышленник может легко завладеть ключевой информацией, а также получить полный информационный доступ к всей информации в сети.

Основным классификационным признаком для средств управления информацией является тип функции управления.[3]

Заключение

Человечество быстро входит в новейшую эпоху использования информации, поскольку самым существенным образом начали использоваться все составные части жизнедеятельности как отдельных людей, так и всего социума.

В нынешнем обществе разные уровни информатизации людей характеризуют также общий уровень развития и государства в целом.

В нынешнее время разные специалисты именуют столетием компьютерных технологий. Повсеместное кардинальное воздействие также касается и самих институтов общества, разных государственных структур, науки, экономической, образовательной, социальной сферы, культуры, а также и самого образа жизни человечества.

Многие развивающиеся страны уже давно осознали в полной мере все положительные преимущества, что несет за собой распространение и развитие разнообразных коммуникационных и информационных технологий (ИТ).

Отметим также, что не вызывает сомнения не у кого тот факт, что быстрое движение к информационному типу общества является путем в светлое будущее для всей нашей цивилизации.

Нынешняя жизнь вообще немыслима и без любого эффективного управления. Особенно важнейшей категорией являются инновационные системы для обработки данных, от которых и зависит во многом самая непосредственная эффективность работы в любом предприятии или учреждении.

Проблема обеспечения полной и качественной защиты информации является одной из самых важных при построении мощной структуры учреждения на основании ЭВМ.

В курсовой работе рассмотренные методы обеспечения ИБ охватывают как физическую защиту данных, а также безопасность системных программ, так и защиту от разного рода несанкционированного доступа к хранимой информации, передаваемой по проводным и беспроводным линиям связи.

Таким образом, в основные понятия защиты данных также включаются все вопросы по хранению целостности данных, а также управления доступа к ним (или санкционированность).

Информационная безопасность может относится к сектору технологий, что развиваются очень быстрыми темпами. Всему этому значительно способствуют как

уровень прогресса в информационных технологиях, а также противоборство так называемых «нападающих» и «защищающихся».

В работе выполнены такие задачи:

– рассмотрены основные понятия по теории информационной безопасности;

– описаны угрозы ИБ в зависимости от источников и мотивации;

– дана характеристика типам воздействий, которые представляют угрозу в вычислительных системах;

– рассмотрены организационно-правовые и технические средства защиты данных;

– описаны криптографические и аппаратно-программные средства защиты данных.

Список использованных источников

- Анин Б. Защита компьютерной информации. Серия "Мастер". - СПб.: БХВ-Петербург, 2014. – 250 с.
- Анин Б. Ю. Защита компьютерной информации. – СПб.:"BHV-Санкт-Петербург" – 2016. –384 с.
- Бабаш А.В. Криптография. - М.: Изд-во "СОЛОН-Пресс", 2014. – 340 с.
- Бабенко Л.К. Современные алгоритмы блочного шифрования и методы их анализа. - М.: Гелиос АРВ, 2016.-376 с., ил.
- Ворона В.А. Системы контроля и управления доступом, издательство: Политехника, 2014. – 236 с.
- Галатенко В. А. Информационная безопасность. –М.: Финансы и статистика, 2014. –158 с.
- Галатенко В.А. Стандарты информационной безопасности. 2-е изд. Курс лекций. Учебное пособие", издательство: ИНТУИТ.РУ, 2014. – 250 с.
- Галицкий, А.В. Защита информации в сети - анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. - М.: ДМК Пресс, 2016. - 615 с.
- Герасименко В. А. Защита информации в автоматизированных системах обработки данных кн. 1.-М.: Энергоатомиздат, 2016.-400с.
- Емельянова, Н. З. Защита информации в персональном компьютере / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2015. - 368 с.
- Защита информации. - М.: Горячая линия - Телеком, 2015. - 176 с.

- Защита информации в телекоммуникационных системах / Г.Ф. Конахович и др. - М.: МК-Пресс, 2015. - 288 с.
- Конеев И. Р. Информационная безопасность предприятия.-СПб.: БХВ-Петербург, 2017.- 752с.:ил.
- Кухарев Г.А. Методы и средства идентификации, издательство: Политехника, 2015.–368 с.
- Лапонина О.Р. Криптографические основы безопасности. - М.: Изд-во "Интернет-университет информационных технологий - ИНТУИТ.ру", 2015. – 250 с.