Создание комплексной системы защиты информации

Лекция

Ревизия: 0.1

Последняя модификация: Vlad Kovtun

Дата последней модификации: 04.01.2011 15:00:00

История изменений

28.11.2009 – Версия 0.1. Первичный документ. Владислав Ковтун

Содержание

Лекция 7. Создание комплексной системы защиты информации

Вопросы

- Понятия.
- Системность подхода.
- Основные трудности.
- Основные правила.
- Защищенная информационная система и система защиты информации.
- Как обеспечить сохранность информации.

Понятия

Вопросы организации защиты информации должны решаться уже на стадии предпроектной разработки ИС.

Опыт проектирования систем защиты еще не достаточен. Однако уже можно сделать некоторые обобщения. Погрешности защиты могут быть в значительной мере устранены, если при проектировании учитывать следующие основные **принципы построения системы защиты:**

- ***Простота механизма защиты.*** Этот принцип общеизвестен, но не всегда глубоко осознается. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты недолжно быть связано со знанием специальных языков или с выполнением трудоемких действий при обычной работе законных пользователей.
- ***Постоянство защиты.*** Надежный механизм, реализующий это требование, должен быть постоянно защищен от несанкционированных изменений. Ни одна компьютерная система не может рассматриваться как безопасная, если основные аппаратные и программные механизмы, призванные обеспечивать безопасность, сами являются объектами несанкционированной модификации или видоизменения.
- ***Всеобъемлющий контроль.*** Этот принцип предполагает необходимость проверки полномочий любого обращения к любому объекту и лежит в основе системы защиты.
- ***Несекретность проектирования.*** Механизм защиты должен функционировать достаточно эффективно даже в том случае, если его структура и содержание известны злоумышленнику. Не имеет смысла засекречивать детали реализации системы защиты, предназначенной для широкого использования. Эффективность защиты не должна зависеть от того, насколько опытны потенциальные нарушители. Защита не должна обеспечиваться только секретностью структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно способствовать ее преодолению (даже автору).
- ***Идентификация.*** Каждый объект ИС должен однозначно идентифицироваться. При попытке получения доступа к информации решение о санкционировании его следует принимать на основании данных претендента и определения высшей степени секретности информации, с которой ему разрешается работать. Такие данные об идентификации и полномочиях должны надежно сохраняться и обновляться компьютерной системой для каждого активного участника системы, выполняющего действия, затрагивающие ее безопасность.

Пользователи должны иметь соответствующие полномочия, объекты (файлы) — соответствующий гриф, а система должна контролировать все попытки получения доступа.

- ***Разделение полномочий.*** Применение нескольких ключей защиты. Это удобно в тех случаях, когда право на доступ определяется выполнением ряда условий.
- ***Минимальные полномочия.*** Для любой программы и любого пользователя должен быть определен минимальный круг полномочий, необходимых для работы.
- ***Надежность.*** Система ЗИ должна иметь механизм, который позволил бы оценить обеспечение достаточной надежности функционирования СЗИ (соблюдение правил безопасности, секретности, идентификации и отчетности). Для этого необходимы выверенные и унифицированные аппаратные и программные

средства контроля. Целью применения данных механизмов является выполнение определенных задач методом, обеспечивающим безопасность.

Максимальная обособленность механизма защиты означает, что защита должна быть отделена от функций управления данными.

Защита памяти. Пакет программ, реализующих защиту, должен размещаться в защищенном поле памяти, чтобы обеспечить системную локализацию попыток проникновения извне. Даже попытка проникновения со стороны программ операционной системы должна автоматически фиксироваться, документироваться и отвергаться, если вызов выполнен некорректно.

Удобство для пользователей: схема защиты должна быть в реализации простой, чтобы механизм защиты не создавал для пользователей дополнительных трудностей.

Контроль доступа на основании авторизации пользователя по его физическому ключу и личному PIN-коду. Это обеспечивает защиту от атак неавторизованных пользователей на доступ:

- к ресурсам ПК;
- к областям HD ПК;
- к ресурсам и серверам сети;
- к модулям выполнения авторизации пользователей.

Авторизация пользователя на основании физического ключа позволяет исключить непреднамеренную дискредитацию его прав доступа.

Отчетность. Необходимо защищать контрольные данные от модификации и несанкционированного уничтожения, чтобы обеспечить обнаружение и расследование выявленных фактов нарушения безопасности. Надежная система должна сохранять сведения о всех событиях, имеющих отношение к безопасности, в контрольных журналах. Кроме того, она должна гарантировать выбор интересующих событий при проведении аудита, чтобы минимизировать стоимость аудита и повысить эффективность анализа. Наличие программных средств аудита или создание отчетов еще не означает ни усиления безопасности, ни наличия гарантий обнаружения нарушений.

Доступность к исполнению только тех команд операционной системы, которые не могут повредить операционную среду и результат контроля предыдущей аутентификации.

Наличие механизмов защиты от:

- несанкционированного чтения информации;
- модификации хранящейся и циркулирующей в сети информации;
- навязывания информации;
- несанкционированного отказа от авторства переданной информации.

Системный подход к защите информации предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенных для обеспечения безопасности ИС.

Возможность наращивания защиты. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Комплексный подход предполагает согласованное применение разнородных средств защиты информации.

Адекватность — обеспечение необходимого уровня защиты (определяется степенью секретности подлежащей обработке информации) при минимальных издержках на создание механизма защиты и обеспечение его функционирования. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и масштаб возможного ущерба были бы приемлемыми (задача анализа риска).

Минимизация привилегий в доступе, предоставляемых пользователям, т.е. каждому пользователю должны предоставляться только действительно необходимые ему права по обращению к ресурсам системы и данным.

Полнота контроля — обязательный контроль всех обращений к защищаемым данным.

Наказуемость нарушений. Наиболее распространенная мера наказания — отказ в доступе к системе.

Экономичность механизма — обеспечение минимальности расходов на создание и эксплуатацию механизма.

Принцип системности сводится к тому, что для обеспечения надежной защиты информации в современных ИС должна быть обеспечена надежная и согласованная защита во всех структурных элементах, на всех технологических участках автоматизированной обработки информации и во все время функционирования ИС.

Специализация, как принцип организации защиты, предполагает, что надежный механизм защиты может быть спроектирован и организован лишь профессиональными специалистами по защите информации. Кроме того, для обеспечения эффективного функционирования механизма защиты в состав ИС должны быть включены соответствующие специалисты.

Принцип неформальности означает, что методология проектирования механизма защиты и обеспечения его функционирования в основе своей — неформальна. В настоящее время не существует инженерной (в традиционном понимании этого термина) методики проектирования механизма защиты. Методики проектирования, разработанные к настоящему времени, содержат комплексы требований, правил, последовательность и содержание этапов, которые сформулированы на неформальном уровне, т.е. механическое их осуществление в общем случае невозможно.

Гибкость системы защиты. Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важно это свойство в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

Принцип непрерывности защиты предполагает, что защита информации — это не разовое мероприятие и даже не определенная совокупность проведенных мероприятий и установленных средств защиты, а **непрерывный целенаправленный процесс***,* предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС. Разработка системы защиты должна осуществляться параллельно с разработкой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные защищенные информационные системы.

Понятия защиты

На формулирование понятия защиты оказывает влияние большое количество разноплановых факторов, основными из которых выступают:

- влияние информации на эффективность принимаемых решений;
- концепции построения и использования защищенных информационных систем;
- техническая оснащенность информационных систем;
- характеристики информационных систем и их компонентов с точки зрения угроз сохранности информации;
- потенциальные возможности злоумышленного воздействия на информацию, ее получение и использование;
- наличие методов и средств защиты информации.

Развитие подходов к защите информации происходит под воздействием перечисленных факторов, при этом можно условно выделить три периода развития СЗИ:

- *первый* — относится к тому времени, когда обработка информации осуществлялась по традиционным (ручным, бумажным) технологиям;
- *второй* — когда для обработки информации на регулярной основе применялись средства электронно-вычислительной техники первых поколений;
- *третий* — когда использование ИТ приняло массовый и повсеместный характер.

Системность подхода

Генеральным направлением поиска путей защиты информации является неуклонное повышение системности подхода к самой проблеме защиты информации. Понятие системности интерпретировалось прежде всего в том смысле, что защита информации заключается не только в создании соответствующих механизмов, а представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла систем обработки данных при комплексном использовании всех имеющихся средств защиты. При этом все средства, методы и мероприятия, используемые для защиты информации, непременно и наиболее рационально объединяются в единый целостный механизм — систему защиты, которая должна обеспечивать, говоря военным языком, глубокоэшелонированную оборону, причем не только от злоумышленников, но и от некомпетентных или недостаточно подготовленных пользователей и персонала.

В этой системе должно быть, по крайней мере, четыре защитных пояса: внешний, охватывающий всю территорию, на которой расположены сооружения; пояс сооружений, помещений или устройств системы; пояс компонентов системы (технических средств, программного обеспечения, элементов баз данных) и пояс технологических процессов обработки данных (ввод/ вывод, внутренняя обработка и т.п.).

Трудности реализации СЗИ

Основные трудности реализации систем защиты состоят в том, что они должны удовлетворять двум группам противоречивых требований. С одной стороны:

- должна быть обеспечена надежная защита находящейся в системе информации, что в более конкретном выражении формулируется в виде двух обобщенных задач:
  - исключение случайной и преднамеренной выдачи информации посторонним лицам и разграничение доступа к устройствам;
  - и ресурсам системы всех пользователей, администрации и обслуживающего персонала.
- С другой стороны, системы защиты не должны создавать заметных неудобств в процессе работы с использованием ресурсов системы.

В частности должны быть гарантированы:

- полная свобода доступа каждого пользователя и независимость его работы в пределах предоставленных ему прав и полномочий;
- удобство работы с информацией для групп взаимосвязанных пользователей;
- возможности пользователям допускать друг друга к своей информации.

Основные правила защиты

Основные правила, которыми рекомендуют руководствоваться специалисты при организации работ по защите информации, сводятся к следующему:

1. Обеспечение безопасности информации есть непрерывный процесс, состоящий в систематическом контроле защищенности, выявлении узких мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты.
2. Безопасность информации в системе обработки данных может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты.
3. Никакая система защиты не обеспечит безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех правил защиты
4. Никакую систему защиты нельзя считать абсолютно надежной, следует исходить из того, что может найтись такой искусный злоумышленник, который отыщет лазейку для доступа к информации.

С самых первых этапов, т.е. с той поры, когда проблема защиты информации в системах обработки данных стала рассматриваться как самостоятельная, основными средствами, используемыми для защиты, были технические и программные.

Техническими названы такие средства, которые реализуются в виде электрических, электромеханических, электронных устройств. Всю совокупность технических средств принято делить на аппаратные и физические. Под аппаратными средствами защиты понимают устройства, внедряемые непосредственно в аппаратуру обработки данных, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Наиболее известные аппаратные средства, используемые на первом этапе — это схемы контроля информации по четности, схемы защиты полей памяти по ключу, специальные регистры (например, регистры границ поля ЗУ) и т.п.

Физическими средствами названы такие, которые реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранной сигнализации и наблюдения, замки на дверях, ре шетки на окнах и т.п.).

Программные средства защиты, как известно, об разуют программы специально предназначенные для выполнения функций, связанных с защитой информации.

Первоначально программные механизмы защиты включались в состав операционных систем или систем управления базами данных. Этим, видимо, и объясняется, что ***практически все без исключения операционные системы содержат механизмы защиты информации от несанкционированного доступа, а именно:***

- динамическое распределение ресурсов вычисли тельной системы и запрещение задачам пользователей использовать чужие ресурсы;
- разграничение доступа пользователей к ресурсам системы по паролям;
- разграничение доступа к полям оперативной и дол говременной памяти по ключам защиты;
- защита таблицы паролей с помощью так называе мого главного пароля.

Защищенная ИС и система защиты информации

Многие специалисты считают, что точный ответ на вопрос, что же такое "защищенная информационная система", пока не найден.

Существуют следующие представления защищенности ИС:

- это совокупность средств и технологических приемов, обеспечивающих защиту компонентов ИС;
- это минимизация риска, которому могут быть подвергнуты компоненты и ресурсы ИС;
- это комплекс процедурных, логических и физических мер, направленных на предотвращение угроз информации и компонентам ИС.

Защищенной будем называть ИС, в которой реализованы механизмы выполнения правил, удовлетворяющих установленному на основе анализа угроз перечню требований по защите информации и компонентов этой ИС.

При этом механизмы выполнения указанных правил чаще всего реализуются в виде **системы защиты информации***.*

Следовательно, **под СЗИ будем понимать** совокупность механизмов защиты, реализующих установленные правила, удовлетворяющие указанным требованиям.

Таким образом, список угроз информации определяет основу для формирования требований к защите. Когда такие требования известны, могут быть определены соответствующие правила обеспечения защиты. Эти правила, в свою очередь, определяют необходимые функции и средства защиты, объединенные в комплексную СЗИ.

Можно утверждать, что чем полнее будет список требований к защите и соответствующих правил защиты, тем эффективнее будет СЗИ для данной ИС.

Для того чтобы построить защищенную ИС, целесообразно провести анализ угроз информации, составить перечень требований к защите, сформулировать правила организации непосредственной защиты и реализовать их выполнение путем создания комплексной СЗИ, которая представляет собой действующие в единой совокупности законодательные, организационные, технические и другие способы и средства, обеспечивающие защиту важной информации от всех выявленных угроз и возможных каналов утечки.

Как обеспечить сохранность информации?

Как же обеспечить сохранность своей информации? Ведь многообразие вариантов построения информационных систем порождает необходимость создания раз личных систем защиты, учитывающих индивидуальные особенности каждой из них. Вместе с тем, в настоящее время разработано и применяется большое количество технологий,

способов и средств защиты информации, которые необходимо проанализировать и использовать в информационных системах уже сегодня. Это позволит резко сократить утечку сведений конфиденциального характера.

Руководителям следует помнить, что закон Мерфи актуален и для проблем защиты информации. Напомним его содержание:

Если какая-нибудь неприятность может случиться, она случается.

Следствия.

1. Все не так легко, как кажется.

2. Всякая работа требует больше времени, чем вы думаете.

3. Из всех неприятностей произойдет именно та, ущерб от которой больше.

4. Если четыре причины возможных неприятностей заранее устранены, то всегда найдется пятая.

5. Предоставленные самим себе, события имеют тенденцию развиваться от плохого к худшему.

6. Как только вы принимаетесь делать какую-то ра боту, находится другая, которую надо сделать еще раньше.

7. Всякое решение плодит новые проблемы.

Приступая к работе по созданию защищенной ИС, желательно в собственном представлении создать об раз Вашей ИС в любом удобном для простого понимания виде. Попробуйте включить фантазию в этот процесс.

Прежде чем начать разговор о возможных путях организации зашиты информации (ЗИ), необходимо определиться, имеется ли у Вас информация, которую нельзя не защищать; это важно, поскольку, как правило, ЗИ потребует дополнительных средств и достаточно больших.

СЗИ — довольно дорогостоящее удовольствие (а чаще необходимость). И если после долгих колебаний и споров решено, что в ИС имеет место информация, которую необходимо защищать, не расстраивайтесь. Смело идите вперед.

Далее необходимо определить конкретные сведения, подлежащие защите, для чего и от кого их защищать, а так же степень надежности такой защиты — проделать это не сложно.

После этого следует выявить потенциальные угрозы и наиболее вероятные каналы утечки информации для конкретных условий. Их может оказаться достаточно много, но не стоит огорчаться, так как злоумышленник не будет их использовать все сразу.

Следующим шагом будет выбор из множества предлагаемых вариантов таких методов, мероприятий и средств, которые можно было бы использовать конкретно в Вашей ИС.

После того как удалось найти конкретные варианты организационных и технических решений, необходимо подсчитать затраты на их реализацию. Вот здесь можно и огорчиться. Сомнения и чувство досады, возникающие в такие моменты — это вполне нормальное явление. Часто при этом всплывают воспоминания о том, как спокойно жилось, пока проблемы защиты ин формации не были Вам знакомы.

Но рано или поздно наступает момент, когда становится ясно: как бы мы этого не хотели, а придется выложить дополнительные средства на организацию защиты своих данных. Было бы неплохо, чтобы такая мысль пришла пораньше, поскольку построить систему защиты информации для готовой (законченной) информационной системы можно лишь путем введения целого ряда ограничений, а это, естественно, снижает эффективность функционирования информационной системы в целом.

Лучше всего анализировать опасности еще на стадии проектирования рабочего места, локальной сети или всей системы, чтобы сразу определить потенциальные потери и установить требования к мерам обеспечения безопасности.

Выбор защитных и контрольных мероприятий на этой ранней стадии требует гораздо меньших затрат, чем выполнение подобной работы с эксплуатируемой компьютерной системой.

Чаще всего бывает достаточно анализа возможных опасностей, чтобы осознать проблемы, которые могут проявиться во время работы. Недаром эксперты по безопасности компьютерных систем часто подчеркивают, что проблемы ЗИ в

значительной степени являются социальными, и если эти проблемы загонять внутрь, они могут "выйти боком". Все усилия и средства по защите информации должны быть объединены в стройную систему защиты информации, работающую по принципу: "копейка рубль бережет".

Современные популярные и доступные широкому кругу пользователей персональные компьютеры в действительности не обеспечивают безопасность информации, поскольку любой, кто имеет доступ к компьютеру, может изменять, читать или копировать данные. Изначально ПК были созданы для решения бытовых и офисных задач и не предназначались для обработки секретной или конфиденциальной информации.

Несколько позднее на базе таких ПК появились локальные сети, а вместе с ними — и "головная боль" от проблем защиты информации. Конечно, решить все эти проблемы непросто. Но, как говорится, вместо того, чтобы хвататься за голову, необходимо просто взяться за ум.

Создание СЗИ можно сравнить с пошивом костюма. При наличии обязательных составляющих (брюки, пиджак, рукава, воротник...) имеется множество фасонов (вариантов покроя), при этом необходимо учитывать индивидуальные особенности каждого заказчика (пропорции тела, вкусы, привычки...). В итоге все стремятся получить удобную, практичную, качественную, красивую, современную вещь.

Серьезная работа по практическому использованию информационных технологий началась сравнительно недавно. Широкий выбор разнообразного аппаратного и программного обеспечения позволяет построить ИС под свои конкретные задачи. Но, как это часто бывает, наблюдается существенный разрыв между тем, что мы имеем в своем распоряжении и тем, что мы можем из этого извлечь... Иначе говоря, компьютер можно использовать не только в качестве неплохой пишущей машинки.

Давно известно, что рыть траншею и прокладывать кабель (или трубы) желательно до того, как в этом месте положат асфальт. Так и СЗИ целесообразно строить одновременно с ИС, начиная с этапа проектирования.

А можно ли сэкономить на своей информационной безопасности? Да, можно! Но стоить это будет дороже!

Основные правила, которыми рекомендуют руководствоваться специалисты при организации работ по защите информации, сводятся к следующему:

1. Обеспечение безопасности информации есть непрерывный процесс, состоящий в систематическом контроле защищенности, выявлении узких мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты.
2. Безопасность информации в системе обработки данных может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств за щиты.
3. Никакая система защиты не обеспечит безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех правил защиты.
4. Никакую систему защиты нельзя считать абсолютно надежной, следует исходить из того, что может найтись такой искусный злоумышленник, который отыщет лазейку для доступа к информации.

Существуют следующие представления защищенности ИС:

- *защищенность* это совокупность средств и технологических приемов, обеспечивающих защиту компонентов ИС;
- *защищенность* это минимизация риска, которому могут быть подвергнуты компоненты и ресурсы ИС;
- *защищенность* это комплекс процедурных, логических и физических мер, направленных на предотвращение угроз информации и компонентам ИС.

Защищенной ИС будем называть ИС, в которой реализованы механизмы выполнения правил, удовлетворяющих установленному на основе анализа угроз перечню требований по защите информации и компонентов этой ИС.

При этом механизмы выполнения указанных правил чаще всего реализуются в виде *системы защиты информации.* Следовательно, *под СЗИ будем понимать* совокупность механизмов защиты, реализующих установленные правила, удовлетворяющие указанным требованиям.

Требования к СЗИ

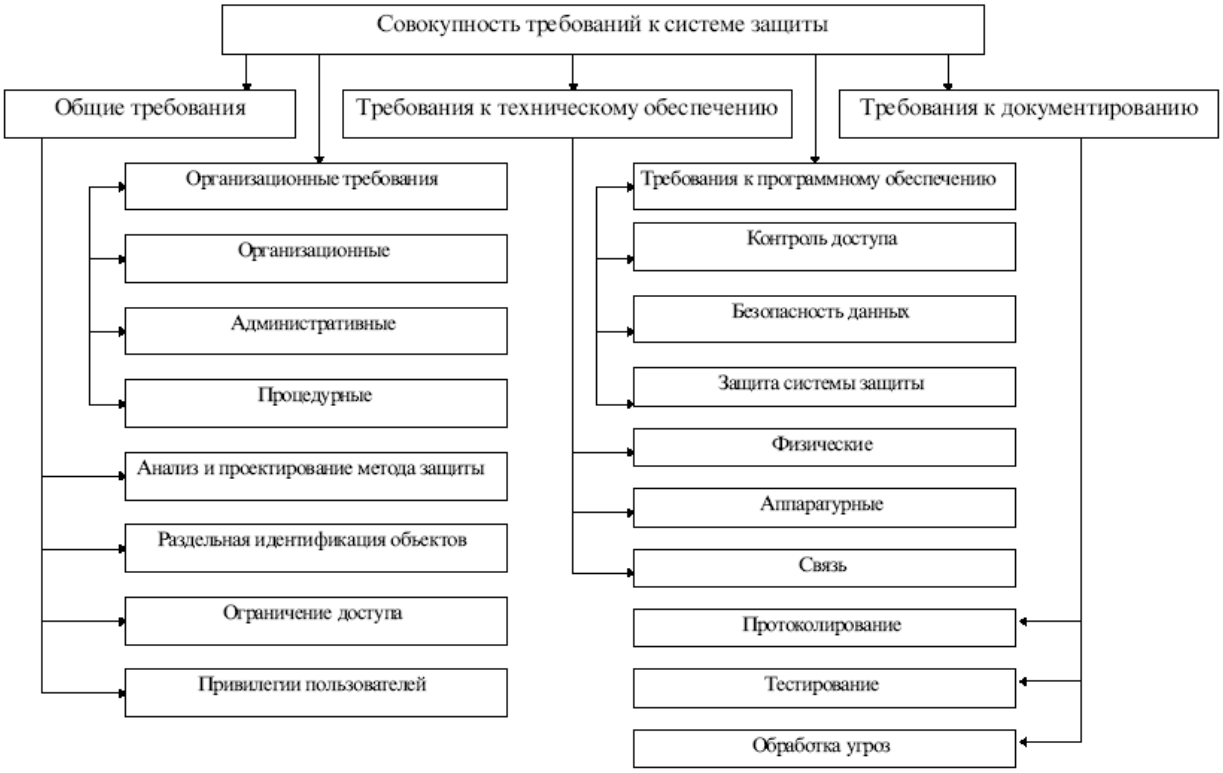

Рис. 1. Совокупность требований к СЗИ

Общие требования

Прежде всего, необходима полная идентификация пользователей, терминалов, программ, а также основных процессов и процедур, желательно до уровня записи или элемента. Кроме того **следует ограничить доступ к информации, используя совокупность следующих способов:**

- иерархическая классификация доступа,
- классификация информации по важности и месту ее возникновения,
- указание ограничений к информационным объектам, например пользователь может осуществлять только чтение файла без права записи в него,
- определение программ и процедур, предоставленных только конкретным пользователям.
- Система защиты должна гарантировать, что любое движение данных идентифицируется, авторизуется, обнаруживается и документируется.

Обычно **формулируются общие требования к следующим характеристикам:**

- способам построения СЗИ либо ее отдельных компонент (к программному, программно-аппаратному, аппаратному);
- архитектуре СВТ и ИС (к классу и минимальной конфигурации ЭВМ, операционной среде, ориентации на ту или иную программную и аппаратную платформы, архитектуре интерфейса);
- применению стратегии защиты;
- затратам ресурсов на обеспечение СЗИ (к объемам дисковой памяти для программной версии и оперативной памяти для ее резидентной части, затратам производительности вычислительной системы на решение задач защиты);
- надежности функционирования СЗИ (к количественным значениям показателей надежности во всех режимах функционирования ИС и при воздействии внешних разрушающих факторов, к критериям отказов);
- количеству степеней секретности информации, поддерживаемых СЗИ;

- обеспечению скорости обмена информацией в ИС, в том числе с учетом используемых криптографических преобразований;
- количеству поддерживаемых СЗИ уровней полномочий;
- возможности СЗИ обслуживать определенное количество пользователей;
- продолжительности процедуры генерации программной версии СЗИ;
- продолжительности процедуры подготовки СЗИ к работе после подачи питания на компоненты ИС;
- возможности СЗИ реагировать на попытки несанкционированного доступа, либо на "опасные ситуации";
- наличию и обеспечению автоматизированного рабочего места администратора защиты информации в ИС;
- составу используемого программного и лингвистического обеспечения, к его совместимости с другими программными платформами, к возможности модификации и т.п.;
- используемым закупаемым компонентам СЗИ (наличие лицензии, сертификата и т.п.).

Организационные требования

Организационные требования к системе защиты предусматривают реализацию совокупности административных и процедурных мероприятий.

Требования по обеспечению сохранности должны выполняться, прежде всего, на административном уровне. *Организационные мероприятия, проводимые с целью повышения эффективности защиты информации, должны предусматривать следующие процедуры:*

- ограничение несопровождаемого доступа к вычислительной системе (регистрация и сопровождение посетителей);
- осуществление контроля за изменением в системе программного обеспечения;
- выполнение тестирования и верификации изменений в системе программного обеспечения и программах защиты;
- организацию и поддержку взаимного контроля за выполнением правил защиты данных;
- ограничение привилегии персонала, обслуживающего ИС;
- осуществление записи протокола о доступе к системе;
- гарантию компетентности обслуживающего персонала;
- разработку последовательного подхода к обеспечению сохранности информации для всей организации;
- организацию четкой работы службы ленточной и дисковой библиотек;
- комплектование основного персонала на базе интегральных оценок и твердых знаний;
- организацию системы обучения и повышения квалификации обслуживающего персонала.

С точки зрения обеспечения доступа к ИС необходимо выполнить следующие процедурные мероприятия:

- разработать и утвердить письменные инструкции на загрузку и остановку работы операционной системы;
- контролировать использование магнитных лент, дисков, карт, листингов, порядок изменения программного обеспечения и доведение этих изменений до пользователя;
- разработать процедуру восстановления системы при отказах;
- установить политику ограничений при разрешенных визитах в вычислительный центр и определить объем выдаваемой информации;

- разработать систему протоколирования использования ЭВМ, ввода данных и вывода результатов;
- обеспечить проведение периодической чистки архивов и хранилищ носителей информации для исключения и ликвидации неиспользуемых;
- поддерживать документацию вычислительного центра в соответствии с установленными стандартами.

Требования к подсистемам защиты информации

В общем случае СЗИ целесообразно условно разделить на подсистемы:

- управления доступом к ресурсам ИС (включает также функции управления системой защиты в целом);
- регистрации и учета действий пользователей (процессов);
- криптографическую;
- обеспечения целостности информационных ресурсов и конфигурации ИС.

Для каждой из них определяются требования в виде:

- перечня обеспечиваемых подсистемой функций защиты;
- основных характеристик этих функций;
- перечня средств, реализующих эти функции.

Подсистема управления доступом должна обеспечивать:

- идентификацию, аутентификацию и контроль за доступом пользователей (процессов) к системе, терминалам, узлам сети, каналам связи, внешним устройствам, программам, каталогам, файлам, записям и т.д.;
- управление потоками информации;
- очистку освобождаемых областей оперативной памяти и внешних накопителей.

Подсистема регистрации и учета выполняет:

- регистрацию и учет: доступа в ИС, выдачи выходных документов, запуска программ и процессов, доступа к защищаемым файлам; передачу данных по линиям и каналам связи;
- регистрацию изменения полномочий доступа, создание объектов доступа, подлежащих защите;
- учет носителей информации;
- оповещение о попытках нарушения защиты.

Криптографическая подсистема предусматривает:

- шифрование конфиденциальной информации.
- шифрование информации, принадлежащей разным субъектам доступа (группам субъектов), с использованием разных ключей.
- использование аттестованных (сертифицированных) криптографических средств.

Подсистема обеспечения целостности осуществляет:

- обеспечение целостности программных средств и обрабатываемой информации,
- физическую охрану средств вычислительной техники и носителей информации,
- наличие администратора (службы) защиты информации в ИС,
- периодическое тестирование СЗИ,
- наличие средств восстановления СЗИ,
- использование сертифицированных средств защиты,

Контроль за целостностью:

- программных средств защиты информации при загрузке операционной среды,
- операционной среды перед выполнением процессов,

- функционального ПО и данных,
- конфигурации ИС,
- оперативное восстановление функций СЗИ после сбоев,
- тестирование средств защиты информации,
- обнаружение и блокирование распространения вирусов,
- резервное копирование программного обеспечения и данных,
- контроль доступа к СВТ, дающий уверенность в том, что только авторизованный пользователь использует имеющиеся рабочие программы и информацию,
- контроль действий с персональной авторизацией, запрещающий операции, которые делают операционную среду уязвимой,
- защиту программного обеспечения, исключающую повреждение инсталлированных программ,
- использование только лицензионного программного продукта с целью обеспечения защиты от встроенных модулей разрушения информационной среды и дискредитации систем защиты;
- защиту коммуникаций для обеспечения недоступности передаваемой информации.

Требования к техническому обеспечению

В этой группе формулируются требования к таким параметрам:

- месту применения средств защиты;
- способам их использования (например, реализация требований по защищенности должна достигаться без применения экранирования помещений, активные средства могут применяться только для защиты информации главного сервера и т.п.);
- размерам контролируемой зоны безопасности информации;
- требуемой величине показателей защищенности, учитывающей реальную обстановку на объектах ИС;
- применению способов, методов и средств достижения необходимых показателей защищенности.
- проведению специсследования оборудования и технических средств, целью которого является измерение показателей ЭМИ;
- проведению спецпроверки технических объектов ИС, целью которой является выявление специальных электронных (закладных) устройств.

Требования к программному обеспечению

Программные средства защиты информации должны обеспечивать контроль доступа, безопасность и целостность данных и защиту самой системы защиты. Для этого ***необходимо выполнить следующие условия по контролю доступа:***

- объекты защиты должны идентифицироваться в явном виде при использовании паролей, пропусков и идентификации по голосу;
- система контроля доступа должна быть достаточно гибкой для обеспечения многообразных ограничений и различных наборов объектов;
- каждый доступ к файлу данных или устройству должен прослеживаться через систему контроля доступа для того, чтобы фиксировать и документировать любое обращение.

Безопасность данных может обеспечиваться следующей системой мероприятий:

- объекты данных идентифицируются и снабжаются информацией службы безопасности. Целесообразно эту информацию размещать не в отдельном каталоге, а вместе с информацией, имеющей метки;
- кодовые слова защиты размещаются внутри файлов, что в значительной мере повышает эффективность защиты;

- доступ к данным целесообразен с помощью косвенных ссылок, например списка пользователей, допущенных владельцем файла к размещенным в нем данным;
- данные и программы могут преобразовываться (кодироваться) внутренним способом для хранения.

Система защиты информации должна быть защищена от воздействия окружающей среды:

- информация по отрицательным запросам не выдается;
- повторные попытки доступа после неудачных обращений должны иметь предел;
- при уменьшении конфигурации системы или при ее тестировании функции защиты сохраняются;
- никакие изменения таблиц безопасности, кроме изменения со специального устройства или пульта управления, не разрешаются.

Требования по применению способов, методов и средств защиты (400)

Рекомендуется применение следующих способов, методов и средств, которые предполагают использование:

- интерфейсов с передачей сигналов в виде последовательного кода и в режиме многократных повторений;
- мультиплексных режимов обработки информации, а также СВТ и системного обеспечения, базирующихся на многоразрядных платформах, интерфейсов с передачей сигналов в виде многоразрядного параллельного кода;
- рациональных способов монтажа, при которых обеспечивается минимальная протяженность электрических связей и коммуникаций;
- технических средств, в состав которых входят устойчивые к самовозбуждению схемы, развязывающие и фильтрующие элементы, комплектующие с низкими уровнями ЭМИ;
- сетевых фильтров для блокирования утечки информации по цепям электропитания, а также линейных (высокочастотных) фильтров для блокирования утечки информации по линиям связи;
- технических средств в защищенном исполнении;
- средств пространственного и линейного «зашумления»;
- средств локального либо общего экранирования;
- способов оптимального размещения технических средств, с целью минимизации контролируемой зоны безопасности информации.

Требования к документированию

Можно выделить три группы требований к документированию системы защиты информации. Это протоколирование, тестирование программ и обработка угроз.

При разработке системы **протоколирования** следует учитывать следующие специфические требования:

- необходимость записей всех движений защищаемых данных;
- возможность воссоздания при необходимости ретроспективы использования защищаемого объекта, для реализации которой обеспечивается запоминание состояний программы и окружающей среды;
- накопление статистики по протоколам использования информации в системе.
- Существенной особенностью **тестирования программ системы** защиты информации должно быть наличие специальной программы генерации ложных адресов, несанкционированных попыток доступа к данным, моделирования сбойных ситуаций и других специфических свойств. При тестировании системы защиты информации необходимо также обратить внимание на тщательную проверку таблиц безопасности, системы паролей и программ доступа.

Система защиты информации должна иметь специальное программное обеспечение обработки угроз, включающее:

- регистрацию событий в системном журнале, защищенном от попыток изменения со стороны программ пользователей;

- использование собранных сведений для анализа качественного решения проблемы защиты информации и разработки мероприятий по ее совершенствованию.

Перечисленные требования и мероприятия по обеспечению сохранности информации показывают, что она связана с решением серьезных математических и технических проблем.

Задача защиты информации в ИС обычно сводится к выбору средств контроля за выполнением программ, имеющих доступ к информации, хранящейся в системе.

Требования к составу проектной и эксплуатационной документации

В состав разрабатываемой документации входят:

- проектная документация разработчика системы (подсистемы, компонента) защиты информации;
- руководство пользователя;
- руководство администратора защиты информации;
- руководство по тестированию системы защиты информации.

Проектная документация

Проектная документация разработчика системы (подсистемы, компонента) защиты информации состоит из описания:

- системы защиты информации;
- концепции защиты;
- модели защиты (формальной или неформальной);
- интерфейса СЗИ и пользователя, а также интерфейсов между отдельными модулями СЗИ;
- применяемых средств защиты;
- результатов анализа и идентификации скрытых каналов передачи информации;
- таблицы соответствия формальных спецификаций v объектных кодов версий программных компонент СЗИ.

Руководство пользователя

Руководство пользователя должно содержать краткое описание механизмов защиты и инструкции по работе с ними в процессе взаимодействия пользователя и ИС

Руководство администратора защиты информации

Руководство администратора защиты информации применяется при выполнении функциональных обязанностей им или сотрудниками службы защиты информации в ИС и должно состоять из таких документов:

- описания контролируемых функций СЗИ;
- инструкции по управлению защитой, управлению и контролю за привилегированными процессами при функционировании ИС;
- описания процедур работы со средствами регистрации;
- инструкции по расшифровке диагностических сообщений и анализу аудиторских файлов;
- инструкции по сопровождению копий программного обеспечения (ПО) СЗИ, проверке их работоспособности и тестированию;
- инструкции по генерации новой версии после модификации;
- описания процедуры старта;
- описания процедур верификации защищенности после старта (сбоев);
- описания процедур оперативного восстановления работоспособности СЗИ.

Руководство по тестированию системы защиты информации

Руководство по тестированию системы защиты информации должно включать документацию разработчика для оценивания защищенности, содержащую полное описание порядка тестирования и тестовых процедур механизмов системы защиты, а также результатов функционального тестирования уровня защищенности информации.

Перечень основных функциональных задач, которые должна решать СЗИ

На основе анализа рассмотренных требований формулируются основные функциональные задачи, которые должна решать СЗИ, например:

- предоставление пользователям права доступа к ресурсам ИС, согласно принятой стратегии безопасности, а также отмена этого права по окончании срока
- действия;
- обеспечение входа в ИС при условии предъявления электронного идентификатора и ввода личного пароля;
- многоуровневое разграничение полномочий пользователей по отношению к ресурсам ИС;
- контроль за запуском процессов и их исполнением;
- контроль за логическим входом пользователей в ИС и доступом к ресурсам;
- управление информационными потоками, автоматическое маркирование ресурсов, создаваемых объектов, экспорта (импорта) информации;
- защита информации при ее передаче по каналам связи;
- регистрация действий пользователей по отношению к ресурсам системы;
- обеспечение целостности информационных ресурсов (в том числе обеспечение антивирусной защиты);
- криптографическая защита ресурсов (шифрование в каналах связи, "прозрачное" шифрование, электронная подпись, криптографическая поддержка других механизмов защиты и т.п.);
- поддержка целостности и работоспособности СЗИ;
- поддержка функций администратора защиты информации в ИС.

Технические требования по защите информации от утечки по каналам ПЭМИН

Объекты защищенных ИС категорируются по степени секретности обрабатываемой (циркулирующей в устройствах ИС) информации и по условиям расположения объекта.

Защита от перехвата секретной информации в непосредственной близости от объекта ИС обеспечивается соблюдением контролируемой зоны вокруг него.

Оценка эффективности мер защиты на этапах проектирования, разработки и эксплуатации объектов ИС по каналам, обусловленным:

- электромагнитными полями в диапазоне частот обрабатываемого сигнала;
- наводками опасных сигналов на цепи питания, линии связи и другие токопроводящие коммуникации, уходящие за границу контролируемой зоны;
- излучениями электромагнитных полей высокочастотных гармонических составляющих обрабатываемого сигнала;
- излучениями электромагнитных полей автогенераторов, входящих в состав технических средств (ТС) производится в соответствии со специальными требованиями и рекомендациями по обеспечению защиты от утечки речевой информации посредством побочных электромагнитных излучений и наводок".

Комплексы и объекты ИС необходимо комплектовать ТС, прошедшими специальные исследования.

Размещение и монтаж оборудования ТС необходимо осуществлять с учетом специальных требований на конкретную систему (комплекс), в которых допускаются ссылки на конструкторские или другие технические документы, прилагаемые к данному техническому средству, а также на действующие стандарты, типовые инструкции и нормативно-методические документы.

Конструкция и алгоритм работы элементов управления системой (комплексом) в различных режимах работы аппаратуры должны затруднять (исключать) возможность ошибочных действий обслуживающего персонала, приводящих к утечке секретной информации.

Требования защиты должны выполняться во всех режимах работы системы, комплекса, объекта, которые могут быть установлены в соответствии с эксплуатационной документацией, при различных положениях переключателей, органов настройки и регулировки аппаратуры, а также при неисправностях технических средств.

Требования по защите от перехвата ПЭМИН

При выборе мест для размещения объектов ИС необходимо строго соблюдать требования по обеспечению размеров контролируемой зоны R. Конкретный состав ТС определяется заказчиком совместно с главным конструктором объекта ИС.

Если на объекте невозможно обеспечить размер контролируемой зоны либо если для размещения отдельных ТС требуется контролируемая зона, большая чем R, заказчику совместно с главным конструктором необходимо проанализировать состав ТС и разделить его на 2 группы устройств, прошедших специальные исследования и удовлетворяющие реальным размерам контролируемой зоны объекта и не удовлетворяющие этим требованиям.

Для устройств второй группы в данном случае и следующем необходимо применять дополнительные меры защиты, которые определяются заказчиком совместно с главным конструктором и головной организацией по ТЗИ на основании категории и вида объекта, реального размера контролируемой зоны и состава ТС.

Если на объекте невозможно обеспечить требуемые минимальные расстояния или если для размещения отдельных ТС необходимо проанализировать состав ТС и разделить его на две группы устройств:

1. устройства, прошедшие специсследования и удовлетворяющие реальным, т.е. максимально возможным для данного объекта, расстоянием до технических средств, имеющих выход за пределы контролируемой зоны;
2. устройства, прошедшие специсследования, но не удовлетворяющие реальным расстояниям.

Рекомендуются такие ***дополнительные меры защиты ТС:***

- установка в незащищенных каналах связи, линиях, проводах и кабелях, выходящих за пределы контролируемой зоны, соответствующих фильтров для защиты высокочастотных ТС;
- прокладка проводов и кабелей в экранирующих конструкциях;

Требования по защите системы заземления объекта ИС

Сопротивление заземлителя объекта ИС не должно превышать 4 Ома. Заземляющее устройство должно размещаться в пределах контролируемой зоны. Защитное заземление объекта ИС не должно иметь выход за пределы контролируемой зоны по экранным оболочкам канальных кабелей, по токопроводящим конструктивным элементам кабелей, металлическим трубопроводам, металлоконструкциям здания, и другими коммуникациями, связанным с системой заземления. Запрещается использовать для системы заземления объекта естественные заземлители (металлические трубопроводы, железобетонные конструкции здания и т.п.), имеющие выход за пределы контролируемой зоны.

В том случае, когда нет возможности удалить заземлитель от подземных коммуникаций либо обеспечить требуемое расстояние от него до границы контролируемой зоны, рекомендуется использовать глубинные заземлители.

При наличии в ТС «схемной земли», отдельного заземлителя для нее создавать не требуется. Шина «схемной земли» должна быть проложена изолированно от защитного заземления и металлоконструкций сооружений и не должна образовывать замкнутых петель. Заземляющие проводники должны быть выполнены из медного провода (кабеля) сечением не менее 10 мм.

Требования по защите систем электроснабжения объекта ИС

Все устройства и кабели электроснабжения объекта ИС, включая трансформаторную подстанцию (ТП) низкого напряжения с заземляющим устройством и средствами защиты системы электроснабжения, необходимо размещать в пределах контролируемой зоны и не ближе 10—15 м от ее границ.

Запрещается подключение потребителей электроэнергии, расположенных за пределами контролируемой зоны.

На универсальных объектах электропитание низкочастотных ТС необходимо осуществлять от разделительных систем типа электродвигатель-генератор, дизель-генератор и других в целях обеспечения гальванической и электромагнитной развязки кабелей электропитания ТС и их металлических оболочек от промышленной сети.

Электропитание высокочастотных ТС на универсальных объектах допускается осуществлять от разделительных систем электроснабжения, либо через помехоподавляющие фильтры.

Электропитание ТС должно осуществляться экранированными (бронированными) кабелями. При невозможности выполнения требований по указанному разносу, электропитание ТС должно осуществляться через помехоподавляющие фильтры или от разделительных систем электроснабжения.

Цепи электропитания ТС на участке от основных технических средств до разделительных систем или помехоподавляющих фильтров должны прокладываться в жестких экранирующих конструкциях. Цепи электропитания от помехоподавляющих фильтров или разделительных систем необходимо прокладывать от ТС на расстоянии не менее R.

При совместной прокладке экранированных кабелей электропитания, развязанных от промышленной сети, с кабелями, имеющими выход за пределы контролируемой зоны, необходимо указанные кабели размещать относительно друг друга на расстоянии, не менее 0,3 м при длине параллельного пробега не более 100 м.

При невозможности выполнения данного требования перечисленные кабели электропитания или кабели, имеющие выход за пределы контролируемой зоны, необходимо прокладывать по всей длине параллельного пробега в жесткой экранирующей конструкции без разноса.

Недопустима прокладка в одной экранирующей конструкции кабелей электропитания, развязанных от промышленной сети, с любыми кабелями, имеющими выход за пределы контролируемой зоны.

Запрещается осуществлять электропитание ТС, имеющих выход за пределы контролируемой зоны, от защищенных источников электроснабжения ТС без установки в цепи электропитания ТС фильтров ФП.

За отсутствием разделительных систем допускается по согласованию с головной организацией по ТЗИ осуществлять питание ТС через машинные преобразователи

При проектировании электроснабжения объектов защищенных ИС необходимо предусмотреть следующее:

- исключить контакт заземлений ТП объекта ИС и питающего центра (ЦРП), расположенного за пределами контролируемой зоны. Для этой цели, питающие высоковольтные кабельные линии между ними должны иметь вставки воздушной линии или кабеля без металлической оболочки на границе контролируемой зоны;
- при необходимости вывода питающих кабелей за пределы контролируемой зоны электропитание должно быть выполнено по схеме с изолированной нейтралью (через разделительный трансформатор) кабелем в пластмассовой оболочке.

При невозможности размещения ТП в пределах контролируемой зоны необходимо предусмотреть отдельную систему заземления объекта ИС, изолированную от заземления ТП.

В соответствии с этим от разделительного устройства к распределительному щиту должны прокладываться четырехжильные кабели с пластмассовой оболочкой. Через четвертую жилу кабеля нейтраль-генератора заземляется на отдельный заземлитель объекта ИС. При этом должен быть выполнен контроль изоляции генератора относительно заземления ТП. Эти требования должны распространяться на всех

потребителей, обеспечивающих работу ИС, машинные преобразователи, используемые для соблюдения специальных требований.

Литература

1. Криптографическая защита информации в АСУ СН. Курс лекций. В.И. Долгов. ХВУ. 1998.

2. Криптографическая защита информации в информационных системах. Курс лекций. И.Д. Горбенко. ХНУРЭ. 2002.

3. В.В. Домарев. Защита информации и безопасность компьютерных систем. К.: Издательство ДиаСофт, 1999. 480 с.

4. В.В. Домарев. Безопасность информационных технологий. Методология создания систем защиты. — К.: ООО "ДС", 2001. 688 с.