Методы защиты информации

1. Классификация методов защиты информации
2. Организационно-правовые методы ЗИ
3. Инженерно-технические методы ЗИ
4. Методы криптографической защиты
5. Программно-аппаратные методы ЗИ

При решении задачи защиты информации в КС необходимо применять так называемый системно-концептуальный подход. В соответствии с ним решение задачи защиты информации должно подразумевать:

- системность целевую, при которой защищенность информации рассматривается как составная неотъемлемая часть ее качества;
- системность пространственную, предполагающую взаимосвязанность защиты информации во всех элементах КС;
- системность временную, предполагающую непрерывность защиты информации;
- системность организационную, предполагающую единство организации всех работ по защите информации в КС и управления ими.

Обеспечение информационной безопасности КС является непрерывным процессом, целенаправленно проводимым на всех этапах ее жизненного цикла с комплексным применением всех имеющихся методов и средств.

Существующие методы и средства защиты информации можно подразделить на четыре основные группы:

- методы и средства организационно-правовой защиты информации;
- методы и средства инженерно-технической защиты информации;
- криптографические методы и средства защиты информации;
- программно-аппаратные методы и средства защиты информации.

Организационно-правовые мероприятия, проводимые в процессе создания и эксплуатации КС предназначены для обеспечения защиты информации. Эти мероприятия должны проводиться при строительстве или ремонте помещений, в которых будут размещаться компьютеры; при проектировании системы, монтаже и наладке ее технических и программных средств; при испытаниях и проверке работоспособности компьютерной системы.

Основой проведения организационных мероприятий является использование и подготовка законодательных и нормативных документов в области информационной безопасности, которые на правовом уровне должны регулировать доступ к информации со стороны потребителей. В российском законодательстве позже, чем в законодательстве других развитых стран, появились необходимые правовые акты.

Система мер по защите информации в широком смысле слова должна строиться исходя из тех начальных условий и факторов, которые, в свою очередь, определяются состоянием устремленности разведок противника либо действиями конкурента на рынке товаров и услуг, направленными на овладение информацией, подлежащей защите.

Это правило действует как на государственном уровне, так и на уровне конкретного предприятия.

Используются два примерно равнозначных определения организационной зашиты информации.

Организационная защита информации — составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Организационная защита информации на предприятии — регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

К основным организационным мероприятиям относят:

1. ***Организацию режима и охраны.*** Их цель - исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей.

2. ***Организацию работы с сотрудниками***, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил ЗИ.

3. ***Организацию работы с документами и документированной информацией***, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение.

4. ***Организацию использования ТС средств сбора, обработки, накопления и хранения конфиденциальной информации***.

5. ***Организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты***.

6. ***Организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.***

Основные направления организационной защиты информации приведены на рисунке

Организационно-правовая защита информации является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации предприятия. От полноты и качества решения организационных задач руководством и должностными лицами предприятия зависит эффективность функционирования системы защиты информации в целом. Роль и место организационной защиты информации в общей системе мер, направленных на защиту конфиденциальной информации предприятия, определяются исключительной важностью принятия руководством своевременных и верных управленческих решений с учетом имеющихся в его распоряжении сил, средств, методов и способов защиты информации и на основе действующего нормативно-методического аппарата.

К ***правовым методам обеспечения информационной безопасности РФ*** относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности РФ.

Наиболее важными направлениями этой деятельности являются:

- внесение изменений и дополнений в законодательство РФ, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности РФ, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась Россия, и противоречий между федеральными законодательными актами и законодательными актами субъектов Российской Федерации, а также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности РФ;

- законодательное разграничение полномочий в области обеспечения информационной безопасности РФ между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;
- разработка и принятие нормативных правовых актов РФ, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;

- уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России;
- законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;
- определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций;
- создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.

Техническая защита информации - одна из основных компонент комплекса мер по защите информации.

Техническая защита информации включает комплекс по обеспечению безопасности информации техническими средствами. Она решает следующие задачи:

1. Предотвращение проникновения злоумышленника к источникам информации с целью ее уничтожения, хищения или изменения.
2. Защита носителей информации от уничтожения в результате воздействия стихийных сил и прежде всего, пожара и воды (пены) при его тушении.
3. Предотвращение утечки информации по различным техническим каналам.

Способы и средства решения первых двух задач не отличаются от способов и средств защиты любых материальных ценностей, третья задача решается исключительно способами и средствами инженерно-технической защиты информации.

Для обеспечения эффективной инженерно-технической защиты информации необходимо определить:

- что защищать техническими средствами в конкретной организации, здании, помещении;
- каким угрозам подвергается защищаемая информация со стороны злоумышленников и их технических средств;
- какие способы и средства целесообразно применять для обеспечения безопасности информации с учетом как величины угрозы, так и затрат на ее предотвращение;
- как организовать и реализовать техническую защиту информации в организации.

Поскольку значительную часть расходов на защиту информации составляют затраты на закупку и эксплуатацию средств защиты, то методология инженерно-технической защиты должна обеспечивать возможность рационального выбора средств защиты.

Следовательно, при решении задач защиты информации объективно существует необходимость учета большого числа различных факторов, что не удается, как правило, сделать на основе здравого смысла. Поэтому основы инженерно-технической защиты должны содержать как теоретические знания, так и методические рекомендации, обеспечивающие решение этих задач.

Принципы технической защиты информации

В основу защиты должны быть положены следующие принципы, аналогичные принципам добывания, а именно:

- непрерывность защиты информации, характеризующая постоянную готовность системы защиты к отражению угроз безопасности информации в любое время;
- активность, предусматривающая прогнозирование действий злоумышленника, разработку и реализацию опережающих мер по защите;
- скрытность, исключающая ознакомление посторонних лиц со средствами и технологией защиты информации;
- целеустремленность, предполагающая сосредоточение усилий по предотвращению угроз наиболее ценной информации;
- комплексное использование различных способов и средств защиты информации, позволяющая компенсировать недостатки одних достоинствами других.

Следующая группа принципов характеризует основные профессиональные подходы к организации защиты информации:

- соответствие уровня защиты ценности информации;
- гибкость защиты;
- многозональность защиты, предусматривающая размещение источников информации в зонах с контролируемым уровнем ее безопасности;
- многорубежность защиты информации на пути движения злоумышленника или распространения носителя.

Криптографические методы обеспечения информационной безопасности.

Шифрование — это способ изменения сообщения или другого документа, обеспечивающее искажение (сокрытие) его содержимого. (Кодирование – это преобразование обычного, понятного, текста в код. При этом подразумевается, что существует взаимно однозначное соответствие между символами текста(данных, чисел, слов) и символьного кода – в этом принципиальное отличие кодирования от шифрования. Часто кодирование и шифрование считают одним и тем же, забывая о том, что для восстановления закодированного сообщения, достаточно знать правило подстановки(замены).

Для восстановления же зашифрованного сообщения помимо знания правил шифрования, требуется и ключ к шифру. Ключ понимается нами как конкретное секретное состояние параметров алгоритмов шифрования и дешифрования. Знание ключа дает возможность прочтения секретного сообщения. Впрочем, как вы увидите ниже, далеко не всегда незнание ключа гарантирует то, что сообщение не сможет прочесть посторонний человек.). Шифровать можно не только текст, но и различные компьютерные файлы – от файлов баз данных и текстовых процессоров до файлов изображений.

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);
- знание алгоритма шифрования не должно влиять на надежность защиты;
- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
- структурные элементы алгоритма шифрования должны быть неизменными;
- дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;

- длина шифрованного текста должна быть равной длине исходного текста;
- не должно быть простых и легко устанавливаемых зависимостью между ключами, последовательно используемыми в процессе шифрования;
- любой ключ из множества возможных должен обеспечивать надежную защиту информации;
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Программно-аппаратные средства обеспечения информационной безопасности.

Программно-аппаратная защита используется для защиты программного обеспечения от несанкционированного (неавторизованного) доступа и нелегального использования. Защитный механизм программным образом опрашивает специальное устройство, используемое в качестве ключа, и работает только в его присутствии. Таким образом, механизм программно-аппаратной защиты содержит две составляющие:

1.аппаратное устройство(аппаратная часть);

2.программный модуль(программная часть).

Поэтому обычно говорят о системах программно-аппаратной защиты.

Очевидно, что стоимость такого механизма превышает стоимость программной защиты, причем стоимость аппаратной части, как правило, превышает стоимость программной части. По этой причине программно-аппаратная защита считается привилегией корпоративных заказчиков, так как для индивидуального пользователя часто неприемлема с экономической точки зрения.

Система защиты от несанкционированного доступа к данным реализована таким образом, что осуществляет проверку легальности пользователя при работе с программным обеспечением и тем самым косвенно препятствует и незаконному использованию программы.

Кроме того, современные аппаратные устройства (ключи), помимо информации о законном пользователе, могут содержать также информацию о программном продукте. А системы программно-аппаратной защиты, кроме аутентификации пользователя, могут производить аутентификацию приложения.

Способы взлома программно-аппаратной защиты

На практике в основном применяются два способа взлома программно-аппаратной защиты:

1. Отключение (взлом) программной части защиты.
2. Эмулирование электронного ключа.

Первый способ взлома заключается в удалении (модификации) из защищенного приложения полностью или частично кодов, связанных с механизмом защиты. Например, иногда достаточно удалить из программы команды опроса электронного ключа и/или команды сравнения с эталоном. Очевидно, что большинство из рассмотренных выше методов взлома программной защиты могут быть использованы для взлома программной части программно-аппаратной защиты

Эмулирование электронного ключа - это способ взлома путем эмулирования программными или аппаратными средствами работы электронного ключа.

Эмулятор - программа, выполняющая функции, обычно реализуемые некоторым внешним устройством.

Программа-эмулятор реализована таким образом, что возвращает защищенному приложению «правильные» ответы на все обращения к электронному ключу. В результате получается электронный ключ, реализованный только на программном уровне.

Для защиты от эмуляции электронного ключа рекомендуется использовать хаотический порядок обмена информацией между защищенным приложением и электронным ключом

Обычно эмулятор взаимодействует с защищенным приложением либо через точку входа API вызова ключа, либо подменой драйвера работы с ключом.

Для противодействия эмуляции через точку входа рекомендуется контролировать целостность соответствующего фрагмента программы и/или зашифровать его. Специалисты рекомендуют наряду с явными обращениями к ключу реализовывать и скрытые вызовы.

Для противодействия эмуляции с помощью подмены драйвера работы с ключом специалисты также рекомендуют контролировать целостность драйвера, например, с помощью электронной цифровой подписи.