МИНИСТЕРСТВО РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИИ И КОМУНИКАЦИИ РЕСПУБЛИКИ УЗБЕКИТСАН

НУКУССКИЙ ФИЛИАЛ ТАШКЕНСТКОГО УНИВЕРСИТЕТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИИ

Факультет: Компьютерный инжиниринг
Группа: 201-15 КИ рус (2в КИ)

Самостоятельная работа

По предмету:_____

На тему:_ Комплексный подход к обеспечению информационной безопасности

Сдал :

_____

Принял(а) :

_____

Содержание

Введение

Проблема защиты информации: надежное обеспечение ее сохранности и установление статуса использования - является одной из важнейших проблем современности.

Еще 25-30 лет назад задача защиты информации могла быть эффективно решена с помощью организационных мер и отдельных программно - аппаратах средств разграничения доступа и шифрования. Появление персональных ЭВМ, локальных и глобальных сетей, спутниковых каналов связи, эффективных технической разведки и конфиденциальной информации существенно обострило проблему защиты информации.

Особенностями современных информационных технологий являются:

- Увеличение числа автоматизированных процессов в системах обработки данных и важности принимаемых на их основе решений;
- Территориальная распределенность компонентов компьютерной системы и передача информации между этими компонентами;
- Усложнение программных и аппаратных средств компьютерных систем;
- Накопление и длительное хранение больших массивов данных на электронных носителях;
- Интеграция в единую базу данных информацию различной направленности различных методов доступа;
- Непосредственный доступ к ресурсам компьютерной системы большого количества пользователей различной категории и с различными правами доступа в системе;
- Рост стоимости ресурсов компьютерных систем.

Рост количества и качества угроз безопасности информации в компьютерных системах не всегда приводит к адекватному ответу в виде создания надежной системы и безопасных информационных технологий. В большинстве коммерческих и государственных организаций, не говоря о простых пользователях, в качестве средств защиты используются только антивирусные программы и разграничение прав доступа пользователей на основе паролей.

1. Комплексный подход к обеспечению информационной безопасности

1.1 Основные понятия

Под *информацией*, применительно к задаче ее защиты понимается сведения о лицах, предметах, фактах, событиях явлениях и процессах независимо от формы их представления. В зависимости от формы представления информация может быть речевой, телекоммуникационной, документированной.

Информационные процессы – процессы сбора, накопления, обработки хранения, распределения и поиска информации.

Информационная система- совокупность документов и массивов документов и информационных технологий.

Информационными ресурсами называют документы или массив документов существующие отдельно или в составе информационной системы.

Процесс создания оптимальных условий для удовлетворения информационных потребностей граждан, организаций, общества и государства называется *информатизацией.*

Информатизация разделяется на открытую и ограниченного доступа.

Информация является одним из объектов гражданского права том числе и прав собственности, владения, пользования. *Собственник* информационных ресурсов, технологий и систем – субъект с правом владения, пользования и распределения указанных объектов. *Владельцем* ресурсов, технологий и систем является субъект с полномочиями владения и пользования указанными объектами. Под пользователем понимается субъект обращающийся к информационной системе за получением нужной информации и пользующегося ею.

К *защищаемой* относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, выдвигаемыми собственником информации.

Под *утечкой* информации понимают неконтролируемое распространение защищенной информации путем ее разглашения, несанкционированного доступа и получение разведчиками. Несанкционированный доступ - получение защищенной информации заинтересованным субъектом с нарушением правилом доступа к ней.

Несанкционированное воздействие на защищенную информацию это воздействие с нарушением правил ее изменения(например подменяя электронных документов). Под *непреднамеренным* воздействием на защищенную информацию понимается воздействие на нее из-за ошибок пользователя, сбой техники, или программных средств, природных явлений и других непреднамеренных воздействий(например уничтожение документа на накопителе на жестком диске).

Целью защиты информации является предотвращение нанесения ущерба пользователю, владельцу или собственнику. Под *эффективностью* защиты информации понимается степень соответствия результатов защиты поставленной цели. *Объектом защиты* может быть информация, ее носитель, информационный процесс, в отношении которого необходимо производить защиту в соответствии с поставленными целями.

Конфиденциальность информации – это известность ее содержания только имеющим, соответствующие полномочия субъект.

Шифрование информации это преобразование информации, в результате, которого содержание информации становится непонятным для субъекта, не имеющего соответствующего доступа. Результат шифрования называется *шифротекстом.*

Под *угрозой* информационной безопасности в компьютерной системе понимают события или действия которые могут вызвать изменения функционирования КС, связанные с нарушением защищенности информации обрабатываемой в ней.

Уязвимость информации – это возможность возникновения на каком либо этапе жизненного цикла КС такого ее состояния при котором создастся условия для реальной угрозы безопасности в ней

Атака это действие предпринимаемое нарушителем, в поиске и использовании той или иной уязвимости. Угрозы могу быть разделены на угрозы независящие от деятельности человека и искусственный угрозы, связанные с деятельностью человека.

Искусственные угрозы в свою очередь делятся на непреднамеренные (ошибки в проектировании, ошибки в работе программных средств) и преднамеренные (несанкционированный доступ, несанкционированные действия).

Результатом реализации угроз может быть утечка, искажение или утрата информации.

1.2. Программные и программно-аппаратные средства обеспечения безопасности информации

К аппаратным средствам защиты информации относятся электронные и электронно-механические устройства, включаемые в состав КС и выполняющие(как самостоятельно, так и при помощи программных средств) некоторые функции по обеспечению безопасности информации.

К основным аппаратным средствам защиты информации относятся:

- Устройства ввода идентифицирующий пользователя информации;
- Устройства шифрования информации;
- Устройства для воспрепятствования несанкционированному включению рабочих станций серверов

Под программными средствами информационной безопасности понимают специальные программные средства, включаемые в состав программного обеспечения КС исключительно для выполнения защитах функций.

К основным программным средствам защиты информации относятся:

- Программы идентификации аутентификации пользователей КС;
- Программы разграничения доступа пользователе к ресурсам КС;
- Программы от несанкционированного доступа , копирования изменения и использования.

Под идентификацией пользователя, применительно к обеспечению безопасности КС, однозначное распознание уникального имени субъекта КС. Аутентификация означает подтверждение того, что предъявленное имя соответствует именно данному субъекту.

К преимуществам программных средств защиты информации относятся:

- простота тиражирования
- Гибкость (возможность настройки на различные условия применения)
- Простота применения
- Практически неограниченные возможности их развития

К недостатка программных средств относятся:

- снижение эффективности КС за счет потребления ее ресурсов, требуемых для функционирования программ защиты.
- Более низкая производительность по сравнению с аналогичными функциями защиты аппаратными средствами
- Пристыкованность многих программных средств(а не встроенность в средства КС)

1.3. Требования к комплексным к комплектным система защиты информации.

Основные требования к комплексной системе защиты информации

- Разработка на основе положений и требований существующих законов, стандартов и нормативно - методических документов по обеспечению информационной безопасности;
- Использование комплекса программно-технических средств и организационных мер по защите КС;
- Надежность, конфигурируемость, производительность;
- Экономическая целесообразность;
- Выполнение на всех этапах жизни обработки информации в КС
- Возможность совершенствования
- Обеспечения разграничения доступа к конфиденциальной информации и отвлечение нарушителя на ложную информацию;

- Взаимодействие с незащищенными КС по установленным для этого правилами разграничения доступа;
- Обеспечение провидения учета и расследования случаев нарушения безопасности;
- не должна вызывать у пользователя психологического противодействия и стремление обойтись без ее средств;
- возможность оценки эффективности ее применения

2.МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Криптографические методы

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом волновала человеческий ум с давних времен. История криптографии - ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры.

С широким распространением письменности криптография стала формироваться как самостоятельная наука. Первые криптосистемы встречаются уже в начале нашей эры. Так, Цезарь в своей переписке использовал уже более менее систематический шифр, получивший его имя.

Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Начиная с послевоенного времени и по нынешний день появление вычислительных средств ускорило разработку и совершенствование криптографических методов.

Почему проблема использования криптографических методов в информационных системах (ИС) стала в настоящий момент особо актуальна?

С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц.

С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем еще недавно считавшихся практически не раскрываемыми.

Проблемой защиты информации путем ее преобразования занимается криптология (kryptos - тайный, logos - наука). Криптология разделяется на два направления - криптографию и криптоанализ. Цели этих направлений прямо противоположны.

Криптография занимается поиском и исследованием математических методов преобразования информации.

Сфера интересов криптоанализа - исследование возможности расшифровывания информации без знания ключей.

Современная криптография включает в себя четыре крупных раздела:

Симметричные криптосистемы.

Криптосистемы с открытым ключом.

Системы электронной подписи.

Управление ключами.

Основные направления использования криптографических методов - передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

2.1.1.Системы с открытым ключом

Как бы ни были сложны и надежны криптографические системы - их слабое мест при практической реализации - проблема распределения ключей. Для того, чтобы был возможен обмен конфиденциальной информацией между двумя субъектами ИС, ключ должен быть сгенерирован одним из них, а затем каким-то образом опять же в конфиденциальном порядке передан другому. Т.е. в общем случае для передачи ключа опять же требуется использование какой-то криптосистемы.

Для решения этой проблемы на основе результатов, полученных классической и современной алгеброй, были предложены системы с открытым ключом.

Суть их состоит в том, что каждым адресатом ИС генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется открытым, а другой закрытым. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст в принципе не может быть расшифрован тем же открытым ключом. Дешифрование сообщение возможно только с использованием закрытого ключа, который известен только самому адресату

.

Криптографические системы с открытым ключом используют так называемые необратимые или односторонние функции, которые обладают следующим свойством: при заданном значении *x* относительно просто вычислить значение *f(x),* однако если *y=f(x*), то нет простого пути для вычисления значения *x.*

Множество классов необратимых функций и порождает все разнообразие систем с открытым ключом. Однако не всякая необратимая функция годится для использования в реальных ИС.

В самом определении необратимости присутствует неопределенность. Под необратимостью понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение используя современные вычислительные средства за обозримый интервал времени.

Поэтому чтобы гарантировать надежную защиту информации, к системам с открытым ключом (СОК) предъявляются два важных и очевидных требования:

1. Преобразование исходного текста должно быть необратимым и исключать его восстановление на основе открытого ключа.

2. Определение закрытого ключа на основе открытого также должно быть невозможным на современном технологическом уровне. При этом желательна точная нижняя оценка сложности (количества операций) раскрытия шифра.

Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах. Так, алгоритм RSA стал мировым стандартом де-факто для открытых систем и рекомендован МККТТ.

Вообще же все предлагаемые сегодня криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований:

1. Разложение больших чисел на простые множители.
2. Вычисление логарифма в конечном поле.
3. Вычисление корней алгебраических уравнений.

Здесь же следует отметить, что алгоритмы криптосистемы с открытым ключом (СОК) можно использовать в трех назначениях.

1. Как самостоятельные средства защиты передаваемых и хранимых данных.

2. Как средства для распределения ключей. Алгоритмы СОК более трудоемки, чем традиционные криптосистемы. Поэтому часто на практике рационально с помощью СОК распределять ключи, объем которых как информации незначителен. А потом с помощью обычных алгоритмов осуществлять обмен большими информационными потоками.

3. Средства аутентификации пользователей.

2.1.2.Электронная подпись

В 1991 г. Национальный институт стандартов и технологии (NIST) предложил для появившегося тогда алгоритма цифровой подписи DSA (Digital Signature Algorithm) стандарт DSS (Digital Signature Standard), в основу которого положены алгоритмы Эль-Гамаля и RSA.

В чем состоит проблема аутентификации данных?

В конце обычного письма или документа исполнитель или ответственное лицо обычно ставит свою подпись. Подобное действие обычно преследует две цели. Во-первых, получатель имеет возможность убедиться в истинности письма, сличив подпись с имеющимся у него образцом. Во-вторых, личная подпись является юридическим гарантом авторства документа. Послед-

ний аспект особенно важен при заключении разного рода торговых сделок, составлении доверенностей, обязательств и т.д.

Если подделать подпись человека на бумаге весьма непросто, а установить авторство подписи современными криминалистическими методами - техническая деталь, то с подписью электронной дело обстоит иначе. Подделать цепочку битов, просто ее скопировав, или незаметно внести нелегальные исправления в документ сможет любой пользователь.

С широким распространением в современном мире электронных форм документов (в том числе и конфиденциальных) и средств их обработки особо актуальной стала проблема установления подлинности и авторства безбумажной документации.

В разделе криптографических систем с открытым ключом было показано, что при всех преимуществах современных систем шифрования они не позволяют обеспечить аутентификацию данных. Поэтому средства аутентификации должны использоваться в комплексе и криптографическими алгоритмами.

Иногда нет необходимости зашифровывать передаваемое сообщение, но нужно его скрепить электронной подписью. В этом случае текст шифруется закрытым ключом отправителя и полученная цепочка символов прикрепляется к документу. Получатель с помощью открытого ключа отправителя расшифровывает подпись и сверяет ее с текстом В 1991 г. Национальный институт стандартов и технологии (NIST) предложил для появившегося тогда алгоритма цифровой подписи DSA (Digital Signature Algorithm) стандарт DSS (Digital Signature Standard), в основу которого положены алгоритмы Эль-Гамаля и RSA.

2.2.Методы защиты информации в Internet

Сегодня самая актуальная для Internet тема - проблема защиты информации. Сеть стремительно развивается в глобальных масштабах, и все большее распространение получают системы внутренних сетей (intranet, интрасети). Появление на рынке новой огромной ниши послужило стимулом как для пользователей, так и для поставщиков сетевых услуг к поиску путей повышения безопасности передачи информации через Internet.

Проблема безопасности в Internet подразделяется на две категории: общая безопасность и вопросы надежности финансовых операций. Успешное разрешение проблем в сфере финансовой деятельности могло бы открыть перед Internet необозримые перспективы по предоставлению услуг для бизнеса. В борьбу за решение этой проблемы включились такие гиганты в области использовани кредитных карточек, как MasterCard и Visa, а также лидеры компьютерной индустрии Microsoft и Netscape. Все это касается "денежных" дел; наша же статья посвящена проблеме общей безопасности.

Задача исследований в этой области - решение проблемы конфиденциальности. Рассмотрим для примера передачу сообщений электронной почты с одного SMTP-сервера на другой. В отдельных случаях эти сообщения просто переписываются с одного жесткого диска на другой как обыкновенные текстовые файлы, т. е. прочитать их смогут все желающие. Образно говоря, механизм доставки электронной почты через Internet напоминает ситуацию, когда постиранное белье вывешивается на улицу, вместо того чтобы отжать его в стиральной машине. Не важно, содержатся ли в послании какая-то финансовая информация или нет; важно следующее - любая пересылаемая по Internet информаци должна быть недоступна для посторонних.

Кроме конфиденциальности пользователей также волнует вопрос гарантий, с кем они сейчас "беседуют". Им необходима уверенность, что сервер Internet, с которым у них сейчас сеанс связи, действительно является тем, за кого себя выдает; будь то сервер World-Wide Web, FTP, IRC или любой другой. Не составляет особого труда имитировать (то ли в шутку, то ли с преступными намерениями) незащищенный сервер и попытаться собрать всю информацию о вас. И, конечно же, поставщики сетевых услуг также хотели бы быть уверенными, что лица, обращающиеся к ним за определенными ресурсами Internet, например, электронной почтой и услугами IRC, действительно те, за кого себя выдают.

2.3.Метод парольной защиты

Законность запроса пользователя определяется по паролю, представляющему собой, как правило, строку знаков. Метод паролей считается достаточно слабым, так как пароль может стать объектом хищения, перехвата, перебора, угадывания. Однако простота метода стимулирует поиск путей его усиления.

Для повышения эффективности парольной защиты рекомендуется:

выбирать пароль длиной более 6 символов, избегая распространенных, легко угадываемых слов, имен, дат и т.п.;

использовать специальные символы;

пароли, хранящиеся на сервере, шифровать при помощи односторонней функции;

файл паролей размещать в особо защищаемой области ЗУ ЭВМ, закрытой для чтения пользователями;

границы между смежными паролями маскируются;

комментарии файла паролей следует хранить отдельно от файла;

периодически менять пароли;

предусмотреть возможность насильственной смены паролей со стороны системы через определенный промежуток времени;

использовать несколько пользовательских паролей: собственно пароль, персональный идентификатор, пароль для блокировки/разблокировки аппаратуры при кратковременном отсутствии и т.п.

В качестве более сложных парольных методов используется случайная выборка символов пароля и одноразовое использование паролей. В первом случае пользователю (устройству) выделяется достаточно длинный пароль, причем каждый раз для опознавания используется часть пароля, выбираемая случайно. При одноразовом использовании пароля пользователю выделяется не один, а большое количество паролей, каждый из которых используется по списку или по случайной выборке один раз. В действительно распределенной среде, где пользователи имеют доступ к нескольким серверам, базам данных и даже обладают правами удаленной регистрации, защита настолько осложняется, что администратор все это может увидеть лишь в кошмарном сне.

2.4.Административные меры защиты

Проблема защиты информации решается введением контроля доступа и разграничением полномочий пользователя.

Распространённым средством ограничения доступа (или ограничения полномочий) является система паролей. Однако оно ненадёжно. Опытные хакеры могут взломать эту защиту, «подсмотреть» чужой пароль или войти в систему путём перебора возможных паролей, так как очень часто для них используются имена, фамилии или даты рождения пользователей. Более надёжное решение состоит в организации контроля доступа в помещения или к конкретному ПК в ЛВС с помощью идентификационных пластиковых карточек различных видов.

Использование пластиковых карточек с магнитной полосой для этих целей вряд ли целесообразно, поскольку, её можно легко подделать. Более высокую степень надёжности обеспечивают пластиковые карточки с встроенной микросхемой – так называемые микропроцессорные карточки (МП – карточки, smart – card). Их надёжность обусловлена в первую очередь невозможностью копирования или подделки кустарным способом. Кроме того, при производстве карточек в каждую микросхему заносится уникальный код, который невозможно продублировать. При выдаче карточки пользователю на неё наносится один или несколько паролей, известных только её владельцу. Для некоторых видов МП – карточек попытка несанкционированного использования заканчивается её автоматическим «закрытием». Чтобы восстановить работоспособность такой карточки, её необходимо предъявить в соответствующую инстанцию.

Установка специального считывающего устройства МП – карточек возможна не только на входе в помещения, где расположены компьютеры, но и непосредственно на рабочих станциях и серверах сети.

3. Защита корпоративной информации.

Однако при решении этой проблемы предприятия часто идут на поводу у компаний-подрядчиков, продвигающих один или несколько продуктов, решающих, как правило, частные задачи. Ниже рассмотрим наиболее общие подходы к комплексному решению задачи обеспечения безопасности информации.

Наиболее типичной ошибкой при построении системы защиты является стремление защитить всё и от всего сразу. На самом деле определение необходимой информации (файлов, каталогов, дисков) и иных объектов информационной структуры, которые требуется защитить – первый шаг в построении системы информационной безопасности. С определения этого перечня и следует начать: следует оценить, во сколько может обойтись потеря (удаление или кража) той или иной базы данных или, например, простой одной рабочей станции в течение дня.

Второй шаг – определение источников угроз. Как правило, их несколько. Выделить источник угроз – значит, оценить его цели (если источник преднамеренный) или возможное воздействие (непреднамеренный), вероятность (или интенсивность) его появления. Если речь идет о злоумышленных действиях лица (или группы лиц), то требуется оценить его организационные и технические возможности для доступа к информации (ведь злоумышленник может быть и сотрудником фирмы).

После определения источника угроз можно сформулировать угрозы безопасности информации. То есть что с информацией может произойти. Как правило, принято различать следующие группы угроз:

- несанкционированный доступ к информации (чтение, копирование или изменение информации, ее подлог и навязывание);
- нарушение работоспособности компьютеров и прикладных программ
- уничтожение информации.

В каждой из этих трех групп можно выделить десятки конкретных угроз, однако пока на этом остановимся. Заметим только, что угрозы могут быть преднамеренными и случайными, а случайные, в свою очередь, естественными (например, стихийные бедствия) и искусственными (ошибочные действия персонала). Случайные угрозы, в которых отсутствует злой умысел, обычно опасны только в плане потери информации и нарушения работоспособности системы, от чего достаточно легко застраховаться. Преднамеренные же угрозы более серьезны с точки зрения потери для бизнеса, ибо здесь приходится бороться не со слепым (пусть и беспощадным в своей силе) случаем, но с думающим противником.

Построение системы защиты полезно проводить с принципами защиты, которые достаточно универсальны для самых разных предметных областей (инженерное обеспечение в армии, физическая безопасность лиц и территорий , и т. д.)

- Адекватность (разумная достаточность). Совокупная стоимость защиты (временные, людские и денежные ресурсы) должна быть ниже стоимости защищаемых ресурсов. Если оборот компании составляет 10 тыс. долларов в месяц, вряд ли есть смысл развертывать систему на миллион долларов (так, же как и наоборот).
- Системность. Важность этого принципа особо проявляется при построении крупных систем защиты. Он состоит в том, что система защиты должна строиться не абстрактно (защита от всего), а на основе анализа угроз, средств защиты от этих угроз, поиска оптимального набора этих средств и построения системы.
- Прозрачность для легальных пользователей. Введение механизмов безопасности (в частности аутентификации пользователей) неизбежно приводит к усложнению их действий. Тем не менее, никакой механизм не должен требовать невыполнимых действий (например, еженедельно придумывать 10-значный пароль и нигде его не записывать) или затягивать процедуру доступа к информации.
- Равностойкость звеньев. Звенья – это элементы защиты, преодоление любого из которых означает преодоление всей защиты. Понятно, что нельзя слабость одних звеньев компенсировать усилением других. В любом случае, прочность защиты (или ее уровня, см. ниже) определяется прочностью самого слабого звена. И если нелояльный сотрудник готов за 100 долларов «скинуть на дискету» ценную ин-

формацию, то злоумышленник вряд ли будет выстраивать сложную хакерскую атаку для достижения той же цели.

- Непрерывность. В общем-то, та же равностойкость, только во временной области. Если мы решаем, что будем что-то и как-то защищать, то надо защищать именно так в любой момент времени. Нельзя, например, решить по пятницам делать резервное копирование информации, а в последнюю пятницу месяца устроить «санитарный день». Закон подлости неумолим: именно в тот момент, когда меры по защите информации будут ослаблены, произойдет то, от чего мы защищались. Временный провал в защите, так же, как и слабое звено, делает ее бессмысленной.
- Многоуровневость. Многоуровневая защита встречается повсеместно, достаточно побродить по руинам средневековой крепости. Зачем защита строится в несколько уровней, которые должен преодолевать как злоумышленник, так и легальный пользователь (которому, понятно, это делать легче)? К сожалению, всегда существует вероятность того, что какой-то уровень может быть преодолен либо в силу непредвиденных случайностей, либо с ненулевой вероятностью. Простая математика подсказывает: если один уровень гарантирует защиту в 90%, то три уровня (ни в коем случае не повторяющих друг друга) дадут вам 99,9%. Это, кстати, резерв экономии: путем эшелонирования недорогих и относительно ненадежных средств защиты можно малой кровью добиться очень высокой степени защиты.

Учет этих принципов поможет избежать лишних расходов при построении системы защиты информации и в то же время добиться действительно высокого уровня информационной безопасности бизнеса.

4. Оценка эффективности систем защиты программного обеспечения

Системы защиты ПО широко распространены и находятся в постоянном развитии, благодаря расширению рынка ПО и телекоммуникационных технологий. Необходимость использования систем защиты (СЗ) ПО обусловлена рядом проблем, среди которых следует выделить: незаконное использование алгоритмов, являющихся интеллектуальной собственностью автора, при написании аналогов продукта (промышленный шпионаж); несанкционированное использование ПО (кража и копирование); несанкционированная модификация ПО с целью внедрения программных злоупотреблений; незаконное распространение и сбыт ПО (пиратство).

Системы защиты ПО по методу установки можно подразделить на системы, устанавливаемые на скомпилированные модули ПО; системы, встраиваемые в исходный код ПО до компиляции; и комбинированные.

Системы первого типа наиболее удобны для производителя ПО, так как легко можно защитить уже полностью готовое и оттестированное ПО (обычно процесс установки защиты максимально автоматизирован и сводится к указанию имени защищаемого файла и нажатию "Enter"), а потому и наиболее популярны. В то же время стойкость этих систем достаточно низка (в зависимости от принципа действия СЗ), так как для обхода защиты достаточно определить точку завершения работы "конверта" защиты и передачи управления защищенной программе, а затем принудительно ее сохранить в незащищенном виде.

Системы второго типа неудобны для производителя П.О, так как возникает необходимость обучать персонал работе с программным интерфейсом (API) системы защиты с вытекающими отсюда денежными и временными затратами. Кроме того, усложняется процесс тестирования П.О и снижается его надежность, так как кроме самого П.О ошибки может содержать API системы защиты или процедуры, его использующие. Но такие системы являются более стойкими к атакам, потому что здесь исчезает четкая граница между системой защиты и как таковым П.О.

Для защиты ПО используется ряд методов, таких как:

- *Алгоритмы запутывания* - используются хаотические переходы в разные части кода, внедрение ложных процедур - "пустышек", холостые циклы, искажение количества реальных параметров процедур ПО, разброс участков кода по разным областям ОЗУ и т.п.
- *Алгоритмы мутации* - создаются таблицы соответствия операндов - синонимов и замена их друг на друга при каждом запуске программы по определенной схеме или случайным образом, случайные изменения структуры программы.

- *Алгоритмы компрессии данных* - программа упаковывается, а затем распаковывается по мере выполнения.
- *Алгоритмы шифрования данных* - программа шифруется, а затем расшифровывается по мере выполнения.
- *Вычисление сложных математических выражений в процессе отработки механизма защиты* - элементы логики защиты зависят от результата вычисления значения какой-либо формулы или группы формул.
- *Методы затруднения дизассемблирования* - используются различные приемы, направленные на предотвращение дизассемблирования в пакетном режиме.
- *Методы затруднения отладки* - используются различные приемы, направленные на усложнение отладки программы.
- *Эмуляция процессоров и операционных систем* - создается виртуальный процессор и/или операционная система (не обязательно реально существующие) и программа-переводчик из системы команд IBM в систему команд созданного процессора или ОС, после такого перевода ПО может выполняться только при помощи эмулятора, что резко затрудняет исследование алгоритма ПО.
- *Нестандартные методы работы с аппаратным обеспечением* - модули системы защиты обращаются к аппаратуре ЭВМ, минуя процедуры операционной системы, и используют малоизвестные или недокументированные её возможности.

ЗАКЛЮЧЕНИЕ

Можно сказать, что не существует одного абсолютно надежного метода защиты. Наиболее полную безопасность можно обеспечить только при комплексном подходе к этому вопросу. Необходимо постоянно следить за новыми решениями в этой области. В крупных организациях я бы рекомендовал ввести должность специалиста по информационной безопасности.

Литература

1. Хореев П.В. «Методы и средства защиты информации в компьютерных системах» 2005 год, издательский центр «Академия»
2. Журнал «СпецХакер №04(41)-2004»
3. Баричев С. «Криптография без секретов»
4. http:\\kaspersky.ru\
5. D. Hsiao, D. Kerr, S. Madnick "Computer Security" Academic Press, 1979.
6. Г. А. Черней, С. А. Охрименко, Ф. С. Ляху "Безопасность автоматизированных информационных систем" Ruxanda, 1996.
7. С. Середа "Программно-аппаратные системы защиты программного обеспечения"