Защита процессов и программ

В этой главе

- *Проблемы безопасности программного обеспечения*
- *Механизмы защиты процессов, процедур и программ обработки данных*
- *Уровни защиты процедур и программ*
- *Защита процедур управления*
- *Защита электронного документооборота*
- *Защита операционных систем*
- *Разграничение доступа пользователей к ресурсам*
- *Инструмент системного аудита*
- *Защита в сетевом информационном сервисе*
- *Ядро безопасности ОС*
- *Технологии VPN для корпоративных пользователей*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Под процессом обработки данных будем понимать установленную последовательность процедур, операций или преобразований информации, реализуемых при функционировании ИС (рис. 12.1).

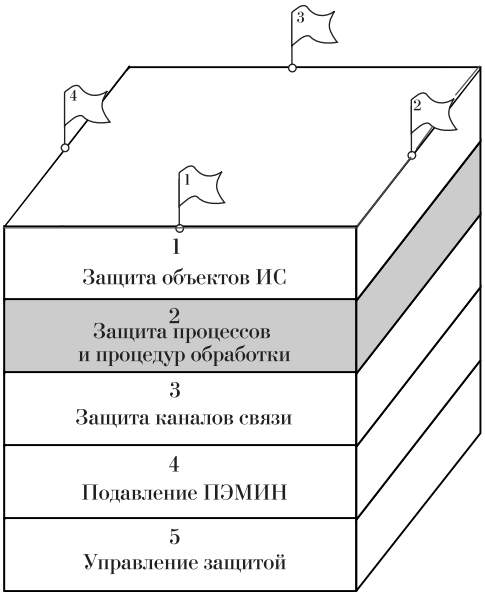


РИСУНОК 12.1

Проблемы безопасности программного обеспечения (020)

Программное обеспечение становится источником уязвимости современных ИС, что порождает новую проблему — обеспечение технологической безопасности программных средств. Опасность нарушения функций программного обеспечения сложных вычислительных систем связана с внесением в программные средства преднамеренных дефектов, именуемых ***программными закладками***, которые служат для целенаправленного скрытого воздействия на техническую или информационную систему.

Программные закладки являются логическим продолжением так называемых *электронных закладок* (скрытых технических устройств), сообщения о которых часто появлялись в прессе во времена "холодной войны", а также результатом осмысления аналогичных возможностей использования программных средств. Чем выше степень компьютеризации и интеллектуализации ИС, тем больше вероятность появления "закладок". Поэтому одной из современных особенностей проектирования и разработки программного обеспечения ИС является необходимость обеспечения его технологической безопасности.

Программная закладка может быть реализована в виде нескольких команд и иметь достаточно сложный и тонкий механизм активизации, настроенный на условия реального боевого применения системы оружия либо на строго определенную комбинацию входных данных. Закладка может быть включена в состав как общего программного обеспечения вычислительной установки, так и специальных (прикладных) программных средств, реализующих алгоритм преобразования информации.

Последствием активизации программных закладок может быть полное или частичное нарушение работоспособности ИС, несанкционированный доступ к защищенной конфиденциальной информации, потеря или искажение информации в специальных банках данных и т.д.

Качество программного средства определяется совокупностью свойств, обуславливающих его состоятельность. Эти свойства проявляются на всех стадиях жизненного цикла — от технического задания до сопровождения и эксплуатации.

Основные проблемы оценки качества программного обеспечения:

- отсутствие общепринятой номенклатуры показателей качества;
- невозможность проведения натурных испытаний программ на всем множестве исходных данных;
- низкая достоверность и недостаточность информации для получения оценок показателей качества и недостаток средств для измерения метрик программ, отсутствие обоснованных требований в числовом выражении и подлежащих проверке;
- отсутствие возможности интерпретации получаемых метрик и оценок показателей качества программ.

Интересно

Опыт использования моделей качества программного обеспечения вынуждает отказаться от построения универсальной номенклатуры показателей качества для всех программных средств. Модели оценки качества должны давать возможность пользователю строить дерево целей (структуру показателей качества) в зависимости от специфики и области применения программного обеспечения.

В развитых странах крайне осторожно относятся к использованию импортных информационных технологий, с полным основанием подозревая наличие в них преднамеренных дефектов, активизируемых при определенном сочетании входных данных.

Положение осложняется также ситуацией, когда нельзя будет однозначно ответить на вопрос, является ли обнаруженная программная конструкция преднамеренной программной закладкой или непреднамеренным случайным программным дефектом. У автора про-

граммной закладки имеется возможность избежать юридической ответственности, используя тонкости разработки программных средств, реализующих особенности алгоритмов и моделей.

В настоящее время для выявления программных закладок и программных дефектов могут быть предложены только дорогостоящие методы контроля исходных текстов программ в сочетании с методами математического моделирования процессов функционирования ИС.

Необходимость защиты программ обработки данных (021)

Необходимость защиты процессов, процедур и программ обработки данных от несанкционированного доступа и использования определяется следующими факторами:

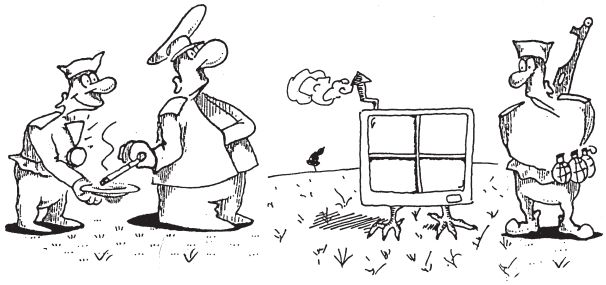
- возможностью случайного или преднамеренного нарушения целостности и истинности вводимой или хранящейся информации на этапе ее ввода в ИС;
- возможностью нарушения целостности, истинности и сохранности информации при ее хранении;
- возможностью утечки, нарушения целостности, истинности и сохранности информации при ее обработке.
- возможностью утечки информации при ее выводе для пользователя, который не должен иметь доступа к данной информации;
- возможностью утечки, нарушения целостности, истинности и сохранности информации при ее передаче между отдельными, территориально удаленными ИС на жестких носителях или по линиям связи.

Перечисленные нарушения происходят в результате случайных или преднамеренных, некорректных (неразрешенных) действий пользователя (санкционированного или несанкционированного для работы в данной ИС).

Указанные нарушения могут возникать в результате воздействия компьютерных вирусов, занесенных в систему ее пользователями с непроверенным программным обеспечением;

Раньше не учитывалось, что пользователи ИС могут вызывать различные ненамеренные ошибки и быть объектом злоупотреблений. Сегодня большая концентрация массивов информации, отсутствие элементарного контроля за ее сохранностью и относительно низкий уровень надежности технических средств вызывают тревогу за сохранность информации.

С появлением ИС, работающих в режиме реального времени, значительно возросло число лиц, имеющих доступ к вычислительным средствам. Это — пользователи, системные и прикладные программисты, обслуживающий и административный персонал.



Значительно возросло число лиц, имеющих доступ к вычислительным средствам...

Совершенствование технологии обработки информации привело к созданию информационных баз данных, содержащих большие объемы разнообразной информации, что также порождает дополнительные требования к обеспечению сохранности информации.

Современные информационные системы обеспечивают одновременный доступ к вычислительным ресурсам для многих пользователей с территориально удаленных терминалов. В связи с этим возникла и новая проблема обеспечения сохранности программ и данных пользователя от неавторизованного (неопознанного) воздействия со стороны других пользователей информационной системы

Механизмы защиты процессов, процедур и программ обработки данных (023)

Механизмы защиты должны контролировать доступ к информационным ресурсам. Диапазон требований к этим механизмам защиты предполагает, с одной стороны, полную изоляцию выполняемой программы от других программ, а с другой —их взаимодействие и совместное использование.

Защита процессов как сетевых ресурсов имеет два аспекта: защита содержания от нелегального просмотра и защита от несанкционированного копирования и распространения. Наиболее надежный механизм для защиты содержания сообщений — криптография.

Защита программ от несанкционированного копирования и распространения может быть обеспечена механизмами защиты, используемыми для обеспечения контроля доступа.

Защита исполняемых файлов**,** разрешенных к применению, от модификации и заражения компьютерными вирусами предназначена для обнаружения заражения компьютерным вирусом любого файла,

разрешенного к применению в операционной среде данного пользователя. Такая защита обеспечивается обязательным контролем попытки запуска любой программы на исполнение, а также контролем содержания запускаемой программы.

Защита от загрузки программного обеспечения несанкционированным пользователем предусматривает исключение возможности свободного доступа со стороны несанкционированного пользователя к ресурсам ИС, к программному обеспечению и информации на ПК. Защита, как правило, обеспечивается аппаратным модулем, устанавливаемым на системную шину ПК, использованием физического ключа для разрешения процесса загрузки и шифрованием служебной информации операционной системы, размещаемой на жестком диске ПК.

Защита от форматирования жесткого диска со стороны пользователей (кроме администратора безопасности), предназначена для исключения вероятности случайного или преднамеренного уничтожения программ и информации со стороны пользователей. Обеспечивается аппаратным модулем, устанавливаемым на системную шину ПК.

Защита от программных закладок предназначена для исключения возможности загрузки в ПК модифицированного программного обеспечения, имеющего в своем теле программные "жучки" для получения повышенного уровня доступа к секретной информации, а также для предотвращения проникновения компьютерных вирусов в информационную систему. Защита обеспечивается аппаратным модулем, устанавливаемым на системную шину ПК, и разрешением загрузки только с системного жесткого диска, установленного в данном ПК.

Средства защиты процедур и программ, могут быть описаны следующим образом:

1. Защита содержания процедур и программ объединяет функции, процедуры и средства защиты, предупреждающие несанкционированное раскрытие конфиденциальных процедур, программ и информации из БД.

2. Средства контроля доступа разрешают доступ к данным только полномочных объектов в соответствии со строго определенными правилами и условиями.

3. Управление потоком защищенных процедур и программ при передаче из одного сегмента БД в другой обеспечивает перемещение процедур и программ вместе с механизмами защиты, присущими исходным данным.

4. Предотвращение возможности выявления конфиденциальных значений из процедур и программ в результате выявления статистически достоверной информации.

5. Контроль согласованности при использовании БД предполагает процедуры, обеспечивающие защиту и целостность отдельных элементов процедур и программ, в частности их значений (зависимость от значений). Успешная реализация таких процедур в ИС означает, что данные в БД всегда логически связаны и значения критических процедур и программ передаются от узла к узлу только при наличии специальных полномочий.

6. Контекстная защита данных, характерная для схем защиты динамических БД, также должна быть включена в состав процедур защиты БД. В этом случае защита отдельного элемента БД в данный момент зависит от проведения всей системы защиты, а также предшествующих операций, выполненных над этим элементом (зависимость от предыстории).

7. Предотвращение создания несанкционированной информации предполагает наличие средств, предупреждающих о том, что объект получает (генерирует) информацию, превышающую уровень прав доступа, и осуществляет это, используя логическую связь между данными в БД.

Уровни защиты процедур и программ (021)

Защита процедур и программ осуществляется на уровнях:

- аппаратуры,
- программного обеспечения,
- данных.

Защита информации на уровнях аппаратуры и программного обеспечения предусматривает управление доступом к таким вычислительным ресурсам, как отдельные устройства ПК, оперативная память, операционная система, специальные служебные программы пользователя. На данном уровне решаются следующие проблемы:

- наличие секретных остатков (в оперативной памяти или на внешнем носителе в неиспользуемых областях остается секретная информация, которая может быть прочитана специальными средствами);
- изменение системных процедур и программ пользователем-нарушителем или программами нарушителями, что может привести к неэффективности всей системы защиты;
- переделка и исправление ошибок, в процессе которых в систему вносятся программы-закладки ("троянские кони", вирусы и т.д.).

Защита информации на уровне данных направлена на:

• защиту информации, передаваемой по каналам связи;

• обеспечение доступа только к разрешенным данным, хранимым в ПК, и выполнение только допустимых действий над ними.

Для защиты информации при передаче целесообразно обратиться к шифрованию: данные шифруются перед вводом в канал связи, а расшифровываются на выходе из него. Шифрование надежно скрывает смысл сообщения.

Наиболее распространенный способ осуществления доступа к информации основан на контроле информационных потоков и разделении субъектов и объектов доступа на классы секретности (категории и уровни, учитывающие полномочия пользователей и семантику информации). Средства контроля должны разрешать поток информации для чтения, если уровень информационного объекта-источника соответствует или не превосходит категорию субъекта-получателя информации, и для записи, если категория субъекта-источника соответствует или превышает уровень секретности информационного объекта.

Средства регистрации, как и средства контроля доступа, относятся к эффективным мерам противодействия несанкционированным действиям. Если же средства контроля доступа предназначены для предотвращения таких действий, то задача регистрации — обнаружить уже совершенные действия или их попытки.

Защита операций над вычислительными ресурсами ИС (023)

С учетом понятий объектов и ресурсов ИС, установлено множество операций и функций, которые могут быть выполнены над ними.

Защита операций над вычислительными ресурсами...

Первая группа операций — это операции инициализации объектов при входе в ИС. К ним относятся: идентификация, подтверждение подлинности и установление сферы действия объекта. После этого объекту разрешается выполнение других операций с включением других объектов: обмен сообщениями, использование услуг электронной почты, проведение телеконференций и т.п. При реализации этих операций и функций выявляются различные аспекты проблем защиты и обеспечения целостности процедур и программ. Функции и средства защиты, относящиеся к активным элементам ИС, целесообразно определить как функции и средства защиты объектов.

Вторая группа операций — это операции передачи процедур и программ и управляющих сообщений по линиям связи. Они также требуют защиты, поскольку линии связи — уязвимый компонент ИС. Соответствующие функции и средства защиты целесообразно определить как функции и средства защиты каналов передачи данных (линий связи).

Третья группа операций — это операции над данными. Они связаны с использованием процедур и программ, их содержанием и способом организации доступа к ним. При анализе проблем защиты эта группа операций выявляет уязвимость информации, которую генерируют объекты ИС, используя данные из различных сетевых БД, доступ к которым ограничен. Соответствующие функции и средства защиты обеспечивают контроль процедур и программ и их защиту, организацию хранения и использования информации; их целесообразно определить как функции и средства защиты баз данных ИС.

Четвертая группа операций — это операции управления процессами, выполняемыми в ИС. Соответствующие средства защиты осуществляют координацию, синхронизацию, обеспечивают целостность и защиту процессов в ИС. Их можно объединить в подсистему управления ИС.

Защита процедур управления (023)

Определение

Используются два понятия — объект и среда. *Объект* — любой активный компонент ИС (как это определено выше), а *среда* — операционное окружение этого объекта в тот интервал времени, когда объект активен и представляет собой некоторое расширенное толкование понятия субъекта.

Поскольку пользователи — активные объекты, то их идентификация и подтверждение подлинности ничем не отличается от соответствующих процедур для любых других компонентов сети. Аналогично, когда обсуждаются средства защиты управления доступом к сегментам БД, можно воспользоваться теми же процедурами для пресечения нелегального доступа к ресурсам сети.

Из числа множества различных процедур управления процессами следует выделить следующие шесть:

- обеспечение защиты ресурсов сети от воздействия неразрешенных процессов и несанкционированных запросов поступающих от разрешенных процессов;
- обеспечение целостности ресурсов при нарушении расписания и синхронизации процессов в сети, ошибочных операций;
- обеспечение защиты ресурсов сети от несанкционированного контроля, копирования или использования (защита программного обеспечения);
- обеспечение защиты при взаимодействии недружественных программных систем (процессов);
- реализация программных систем, не обладающих памятью;
- защита распределения вычислений.

Первые три процедуры связаны с защитой и обеспечением целостности ресурсов ИС (включая процессы), тогда как последние три относятся к организации вычислительных процессов в сети и реализации сетевого окружения.

Механизмы защиты ресурсов ИС должны контролировать доступ к объектам ИС, особенно информационным.

Можно выделить ***четыре уровня требований к таким механизмам:***

- запрещение совместного использования ресурсов (полная изоляция процессов);
- совместное использование собственно ресурсов (программ и сегментов баз данных);
- совместное использование копий ресурсов (программ и сегментов баз данных);
- совместное использование программных систем или подсистем.

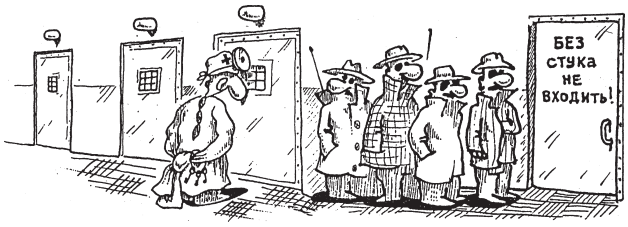
Это обусловлено особенностями реализации вычислительных функций при условии обеспечения защиты и целостности сетевых ресурсов. Процессы в ИС должны поддерживаться подсистемами, корректность функционирования которых проверена и гарантирована.

Защита процессов и процедур передачи информации по каналам связи ИС (023)

Каналы связи — один из наиболее уязвимых компонентов ИС, где можно обнаружить немало потенциально опасных мест, удобных для проникновения в систему.

Действия злоумышленников, направленные на передачу информации по каналам связи, квалифицируются как пассивные и активные вторжения.

В случае ***пассивного вторжения*** злоумышленник только наблюдает за сообщениями, передаваемыми по линиям связи, не нарушая процесса передачи. Такое вторжение называют наблюдением за сообщениями. Даже если непонятны передаваемые данные, злоумышленник может наблюдать за управляющей информацией, которая сопровождает сообщения, и таким образом выявить размещение и идентификаторы объектов ИС. Наконец, он может проверить длину сообщений, время отправления, частоту сеансов связи. Пассивные вторжения связывают либо с анализом трафика, либо с нарушением защиты сеансов связи.



Пассивные и активные вторжения...

Особой формой защиты каналов передачи является двухуровневая защита линий связи, при которой реализуются защита процесса передачи сообщения и шифрование текста сообщения. Тогда, даже если шифрованный текст будет выделен из передаваемого сообщения, для получения исходного текста потребуются дополнительные действия. Это позволяет двум объектам обмениваться секретными сообщениями, вводя злоумышленника, осуществляющего тайное наблюдение, в заблуждение. Такой механизм называется чистым каналом.

Другое, более жестокое требование к защите передаваемых сообщений, состоит в том, что истинные идентификаторы объектов сети должны быть скрыты один от другого и от незарегистрированных пользователей. Такое средство защиты называется цифровым псевдонимом. В этом случае пользователь получает разные идентификаторы для разных соединений, тем самым скрывая истинные идентификаторы не только от злоумышленников, но и от равноправных партнеров.

Средства защиты ИС, необходимые для противодействия пассивным вторжениям в подсистемах связи, состоят в следующем:

- защита содержания сообщения;
- предотвращение возможности анализа трафика;
- чистый канал;
- цифровой псевдоним.

Злоумышленник может организовать активное вторжение посредством различных манипуляций над сообщениями во время соединения. Сообщения могут быть неявно модифицированы, уничтожены, задержаны, скопированы, может быть изменен порядок их следования или время введения в сеть через линию связи. Могут быть также синтезированы ложные сообщения и введены в сеть через канал передачи данных.

В то время как активные вторжения представляют собой комбинации способов, соответствующие механизмы защиты существенно зависят от способа вторжения.

Целесообразно выделить следующие категории активного вторжения:

- воздействие на поток сообщений: модификация, удаление, задержка, переупорядочение, дублирование регулярных и посылка ложных сообщений;
- препятствие передаче сообщений;
- осуществление ложных соединений.

Воздействие на поток сообщений предполагает угрозы процедурам подтверждения подлинности, целостности и порядку следования сообщений во время соединения. В контексте коммуникационных функций ИС подтверждение подлинности сообщения означает, что источник сообщения можно надежно определить, т.е. указать, что полученное сообщение передано данному объекту неким другим объектом в течение сеанса соединения. Целостность сообщения означает, что оно не модифицировалось в процессе передачи, а понятие “порядок следования” означает, что местоположение конкретного сообщения в потоке сообщений может быть проверено.

Вторжение в процедуры установления подлинности может быть осуществлено путем модификации управляющей информации, сопровождающей сообщения, и таким образом сообщения будут отосланы в ложном направлении или будут включать фиктивные сообщения (специально сформированные или сохраненные из предшествующих соединений).

Нарушение целостности может быть вызвано модификацией части данных в сообщении, а нарушение порядка следования — удалением сообщений или изменением информации, управляющей их передачей.

Хотя защита от воздействия на поток сообщений поддерживается коммуникационными протоколами, в данном контексте защита направлена на то, чтобы пресечь умышленное вторжение, а не просто защищаться от случайных непреднамеренных ошибок элементов сети. Поэтому процедура защиты, обеспечивающая противодействие угрозам целостности, порядку следования и подлинности отдельных сообщений, может быть определена как обеспечение целостности потока сообщений.

Препятствие передаче сообщения — вторая категория активных вторжений в подсистемах связи. Она объединяет вторжения, в которых злоумышленник либо удаляет все сообщения во время соединения, либо действует в более мягкой манере, задерживая все сообщения, идущие в одном или обоих направлениях. Такое вторжение может быть организовано нелегальным пользователем, который, генерируя интенсивный трафик фиктивных и подставных сообщений, нарушает циркуляцию регулярных сообщений по линиям связи.

Трудноуловимое различие между атаками на поток сообщений и воспрепятствием их передаче зависит от интенсивности атак и состояния соединения. Например, механизмы защиты, обеспечивающие целостность потока сообщений, могут выявить некоторые вторжения, препятствующие передаче сообщений.

Но если соединение пассивно, т.е. все сообщения разрешаются в любом направлении, то протокол функционирования объекта на одном из концов соединения может оказаться не в состоянии определить, когда следующее сообщение должно поступить от соответствующего объекта. В такой ситуации невозможно определить угрозу с целью воспрепятствовать передаче сообщения, которая полностью прерывала бы поток поступающих сообщений. Чтобы защититься от таких вторжений, необходимы другие механизмы.

Соответствующая процедура защиты сети могла бы быть названа процедурой поддержки непрерывности процесса передачи. Она гарантирует взаимодействующим в ИС объектам невозможность нелегального удаления всех сообщений в процессе соединения без разрушения самого соединения.

Осуществление ложных соединений — третья категория активных вторжений в линии связи. Она объединяет вторжения, в которых злоумышленник либо повторяет записи предшествующих законных соединений, либо делает попытки установить соединение под неправильным идентификатором.

Чтобы предупредить такие вторжения, процедура инициализации соединения должна включать некоторые защищенные механизмы, которые верифицируют целостность соединения (т.е. определяют, что попытка соединения была выполнена в разрешенное время).

Функции, процедуры и средства защиты линий связи ИС от пассивных вторжений:

- конфиденциальность содержания сообщения,
- предотвращение возможного анализа трафика,
- чистый канал,
- цифровые псевдонимы.

Функции, процедуры и средства защиты от активных вторжений:

- поддержание целостности потока сообщений,
- поддержание непрерывности процесса передачи,
- подтверждение подлинности соединения.

Поддержание непрерывности процесса...

Чтобы устранить возможность входа в ИС с не соответствующим идентификатором, соединение должно поддерживать защищенную проверку протоколов объектов на каждом конце соединения (взаимоподтверждение). Хотя верификация идентификатора объекта — сложная проблема, которая может потребовать подтверждения подлинности и контроля защищенности вне ИС, часть проблемы идентификации должна быть решена в рамках ИС. Хотя эта категория вторжений аналогична атакам на поток сообщений, процедура инициализации соединения требует привлечения дополнительных механизмов защиты. Такая процедура защиты может быть названа подтверждением подлинности соединения.

Защита электронного документооборота (023)

Широкомасштабное использование вычислительной техники и телекоммуникационных систем в рамках территориально распределенной сети, переход на этой основе к безбумажной технологии, увеличение объемов обрабатываемой информации, расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационной системы, к их высокой уязвимости.

Особенно остро стоит проблема обеспечения юридической значимости электронных документов, обработка которых осуществляется в информационных системах различного уровня.

В качестве наиболее приемлемого метода целесообразно использовать цифровую подпись электронных документов на основе несимметричного криптографического алгоритма, которая обеспечивает не только юридическую значимость, но также защиту целостности и аутентификацию документов.

Эффективность механизмов защиты информации в значительной степени зависит от реализации ряда принципов.

Во-первых, механизмы защиты должны проектироваться совместно с разработкой информационной системы, что позволяет обеспечить их бесконфликтность, своевременную интеграцию в вычислительную среду и сокращение затрат.

Во-вторых, вопросы защиты следует рассматривать комплексно в рамках единой системы защиты информации (СЗИ) информационной системы. Системный подход обеспечивает адекватную многоуровневую защиту информации, рассматриваемую как комплекс организационно-правовых и технических мероприятий.

Кроме того, при реализации механизмов защиты следует использовать передовые, научно обоснованные технологии защиты, обеспечивающие необходимый уровень безопасности, приемлемость для пользователей и возможность наращивания и модификации СЗИ.

Одним из аспектов обеспечения безопасности информации в ИС является придание юридической силы электронным документам, которые, в отличие от бумажных, более уязвимы и не обладают юридическими реквизитами (подпись, печать и др.).

Криптографические методы, в частности цифровая подпись, позволяют создать уникальные реквизиты электронных документов, практически не подлежащие подделке и создающие основу для признания их юридической значимости.

Методы обеспечения защиты от угроз, связанных с непризнанием участия (023)

Угрозы этой группы характерны тем, что злоумышленниками выступают законные отправитель и получатель. ***В основе механизмов защиты от непризнания участия лежит следующее:*** сторона, пострадавшая от злоумышленных действий другой стороны, должна предоставить доказательство этих действий и при необходимости может обратиться к независимой третьей стороне для проверки.

Отказ от факта формирования сообщения можно предотвратить только с помощью цифровой подписи, однозначно аутентифицирующей создателя сообщения. Кроме того, цифровая подпись может служить основанием для обращения к третьей стороне для решения спорной ситуации. Включение в цифровую подпись временных меток позволяет исключить угрозу предоставления ложных сведений о времени отправки или получения сообщений.

Отказ от факта получения сообщения — более неприятная угроза, которую можно предотвратить с помощью механизмов квитирования сообщений, при этом квитанция также уязвима перед всеми перечисленными угрозами.

Таким образом, для всех угроз электронным документам, важным с точки зрения юридической значимости, существуют достаточно сильные криптографические и иные методы защиты.

Универсальным методом защиты от перечисленной совокупности угроз является цифровая подпись сообщений, которая позволяет обеспечить целостность и аутентификацию сообщений, аутентификацию источника данных и собственно юридическую значимость сообщения.

Правовое обеспечение юридической значимости электронных документов (023)

Как указывалось ранее, юридическая значимость электронных документов обеспечивается реализацией комплекса нормативно-правовых и технических мероприятий. Это один из аспектов нормативно-правового обеспечения защиты информации в целом.

При выборе цифровой подписи в качестве метода обеспечения защиты и юридической значимости электронных документов возникают вопросы правового характера:

- ***Лицензирование деятельности*** по разработке программно-аппаратных средств цифровой подписи направлено на создание условий, при которых право заниматься этими работами предоставлено только организациям, имеющим соответствующее разрешение.
- ***Сертификация программно-аппаратных средств*** цифровой подписи по требованиям безопасности информации. Система сертификации направлена на защиту потребителя продукции и услуг от недобросовестной работы исполнителя. В настоящее время фактически отсутствуют организационно-технические и организационно-методические документы по сертификации средств и комплексов защиты информации, в том числе связанных с криптографическими методами защиты.
- ***Соответствие разрабатываемых средств защиты требованиям к защите***, стандартам и другим нормативным документам. Круг нормативных и концептуальных документов в области защиты информации ограничен, а имеющиеся документы не всегда соответствуют современным требованиям. Из стандартов, относящихся к криптографической защите информации, можно назвать стандарт блочного шифрования ГОСТ 28147-89. Нормативно-правовые документы, содержащие термины и определения, концепцию применения и алгоритмы выработки и проверки цифровой подписи отсутствуют.
- ***Наличие нормативно-правового обеспечения*** для решения спорных ситуаций с использованием цифровой подписи в арбитражном суде.

Принципы использования цифровой подписи для защиты электронных документов (023)

Практические методы цифровой подписи основаны на использовании свойств несимметричных криптографических систем, или систем с открытым ключом. В открытой печати несимметричные криптосистемы впервые рассмотрены У.Диффи и М.Хеллманом в 1975 г. В отличие от симметричных криптосистем, в которых для шифрования и дешифрования используется один и тот же секретный ключ, в несимметричных системах для этих целей используются разные ключи, составляющие пару — открытый и секретный ключи.

Несимметричная криптосистема — это совокупности алгоритмов {Ek}k и {Dk}k, k+{K}, представляющих обратимые преобразования

Ek: {M} —> {M} Dk: {M} —> {M}

на конечном пространстве сообщений таких, что:

1) для каждого k+{K}, Ek является обратной величиной Dk;

2) для каждого k+{K} и M+{M}, несложно вычислить алгоритмы Ek и Dk;

3) почти для каждого k+{K}, каждый несложно вычисляемый алгоритм, эквивалентный Dk, невозможно вычислить из Ek;

4) для каждого k+{K} возможно вычислить пары обратных величин Ek и Dk из k.

Из третьего свойства следует, что ключ шифрования Ek можно сделать открытым (несекретным) без угрозы компрометации секретного ключа дешифрования Dk. Криптосистема разделяется на две части — множество шифрующих преобразований и множество дешифрующих преобразований, при этом для заданного элемента из одного множества невозможно найти соответствующий элемент из другого множества. Четвертое свойство гарантирует, что существует выполнимый способ вычисления соответствующих пар обратных преобразований.

В основе несимметричных криптосистем лежат односторонние функции. Функция f — односторонняя, если для любого аргумента x из области определения f несложно вычислить соответствующее значение f(x), и наоборот, почти для всех y из области значений f вычислительно невозможно решить уравнение y = f(x) для любого приемлемого аргумента x. На практике находят применение односторонние функции с лазейкой, т.е. функции, для которых легко найти обратное значение при знании лазейки -дополнительной информации, например ключа дешифрования Dk. Примером таких функций, близких по свойствам к односторонним, является дискретное возведение в степень (обратная функция -отыскание дискретного логарифма), перемножение простых чисел (обратная функция — разложение на простые множители) и ряд других. В основе функций, используемых на практике, лежат вычислительно сложные задачи, сложность которых не доказана.

Как отмечалось, в несимметричной криптосистеме используется ключевая пара: ключи различны, но между ними имеется однозначное математическое соответствие; открытый ключ и алгоритм преобразования известны всем пользователям, секретный ключ хранится его владельцем в тайне. Это обуславливает следующие возможные применения несимметричных криптосистем.

Защита операционных систем (023)

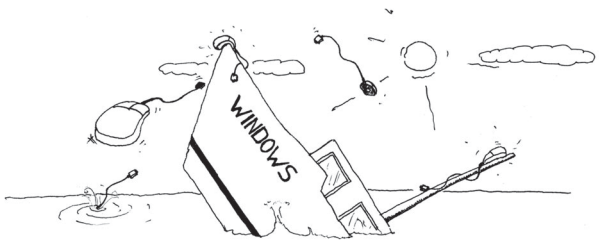
Проблема защиты информации в компьютерных системах напрямую связана с решением двух главных вопросов:

- обеспечение сохранности информации,
- контроль доступа к информации (обеспечение конфиденциальности).

Эти вопросы тесно взаимосвязаны и не могут решаться в отдельности. Сохранность информации означает защиту ее от разрушения и сохранение структуры хранимых данных. Поэтому решение этого вопроса прежде всего означает использование надежных компьютеров и отлаженных программных комплексов.

Система контроля доступа к информации должна обеспечивать надежную идентификацию пользователей и блокировать любые попытки несанкционированного чтения и записи данных. В то же время система контроля не должна снижать производительность работы информационных систем и сужать круг решаемых задач. При этом контроль должен осуществляться как со стороны информационных центров, так и со стороны абонентских ПК, связанных с информационными центрами. Вопросы контроля со стороны информационных центров решаются в каждом случае особо, в зависимости от их конкретной архитектуры. В свою очередь вопрос контроля со стороны абонентских ПК касается не только одиночных ПК, но и ПК, работающих в локальных сетях.

Различные ОС обладают разной степенью защищенности, однако с точки зрения перспективы развития сетей наиболее насущной является задача стыковки различных ОС. Оснащенная механизмами защиты версия ОС Unix может плохо стыковаться с другими ОС, чрезвычайно затрудняя управление безопасностью. Вплоть до того, что две версии одной и той же ОС Unix могут настолько отличаться одна от другой, что более целесообразным решением будет использование некоего третьего пакета защиты. Разумеется, это потребует дополнительных затрат, которые, однако, окупятся благодаря возможности встречной работы различных ОС.



Операционные системы обладают разной степенью защищенности...

Средства обеспечения безопасности ОС могут и должны применяться для защиты информационной системы в целом. Их необходимо дополнить соответственно требованиям к конкретной конфигурации.

Анализировать безопасность ОС необходимо с учетом ее структуры, которая описывается следующим набором уровней:

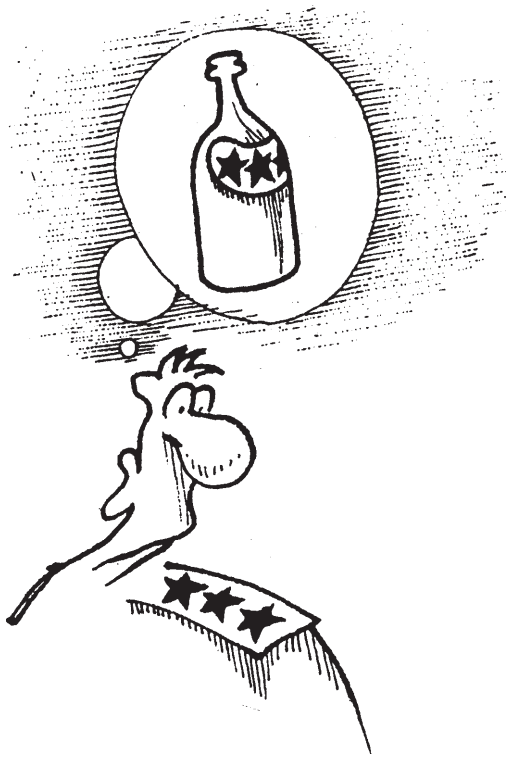
1. ***Внешний уровень***, определяющий взаимодействие информационной системы организации с глобальными ресурсами и системами других организаций. Функционально этот уровень характеризуется, с одной стороны, сетевыми сервисами, предоставляемыми данной организацией, с другой — аналогичными сервисами, запрашиваемыми из глобальной сети. На этом уровне должны ограничиваться как попытки внешних пользователей несанкционированно получить от организации дополнительный сервис, так и попытки собственных пользователей осуществить подобные операции по отношению к внешним сервисам или несанкционированно переслать информацию в глобальную сеть.

2. ***Сетевой уровень*** связан с доступом к информационным ресурсам внутри локальной сети организации. Безопасность информации на этом уровне обеспечивается средствами проверки подлинности пользователей и разграничением доступа к ресурсам локальной сети (аутентификация и авторизация).

3. ***Системный уровень*** связан прежде всего с управлением доступа к ресурсам ОС. Именно на этом уровне происходит непосредственное взаимодействие с пользователями и, самое главное, определяются «правила игры» между информационной системой и пользователем — задается либо изменяется конфигурация системы. В этой связи естественно понимать защиту информации на данном уровне, как четкое разделение, к каким ресурсам ОС какой пользователь и когда может быть допущен. Защите системных ресурсов должно уделяться особое внимание, поскольку несанкционированный доступ к ним может сделать бессмысленными прочие меры безопасности.

4. ***Уровень приложений*** связан с использованием прикладных ресурсов информационной системы. Поскольку именно приложения на содержательном уровне работают с пользовательскими данными, для них нужны собственные механизмы обеспечения информационной безопасности.

Средства защиты, встроенные в ОС, занимают особое место. Их основной задачей является защита информации, определяющей конфигурацию системы, и затем — пользовательских данных. Такой подход представляется естественным, поскольку возможность изменять конфигурацию делает механизмы защиты бессмысленными.



Системные средства аутентификации пользователей...

Системные средства аутентификации пользователей (020)

Первое, что должна проверить операционная система в том случае, если она обладает хотя бы минимальными средствами защиты, — это следует ли ей взаимодействовать с субъектом, который пытается получить доступ к каким-либо информационным ресурсам. Для этого существует список именованных пользователей, в соответствии с которым может быть построена система разграничения доступа.

Имена пользователей представляют собой относительно доступную информацию. В этой связи представляется разумным запросить у потенциального пользователя дополнительную информацию (пароль, удостоверяющий, что он тот, за кого себя выдает). Эта процедура называется аутентификацией. Предполагается, что субъект, способный сообщить системе имя и соответствующий ему пароль, является легальным пользователем. В данной ситуации существенной оказывается политика управления пользовательскими паролями, определяющая правила их назначения, хране-

ния, изменения и другие связанные с этим вопросы. Чем большие возможности по проведению подобной политики предоставляет администратору операционная система, тем больше шансов на то, что парольная аутентификация будет действенным инструментом защиты.

Пароли с течением времени становятся известными. Это вынуждает периодически проводить их замену. Считается, что в информационных системах с низкими требованиями к обеспечению безопасности пароль должен меняться каждые три месяца, а по мере увеличения значимости вопросов, связанных с несанкционированным доступом, указанный срок сокращается до шести недель.

Не менее важно и минимально допустимое время между двумя последовательными изменениями паролей, поскольку такое изменение — типичное действие в случае получения кем-либо несанкционированного доступа к системе либо ресурсам пользователя.

Одной из распространенных угроз безопасности информационной системы является терминал, оставленный пользователем без присмотра во время работы. В качестве контрмеры можно автоматически блокировать доступ либо прерывать сеанс работы в системе спустя некоторое время после прекращения активности пользователя.

Существуют утилиты, позволяющие проводить закрытие экрана автоматически, однако применять их не рекомендуется, поскольку при этом возникают условия для установки программы, эмулирующей закрытие экрана и считывающей пользовательский пароль.

Особую опасность представляет удаленный вход в систему через телефонную сеть. Поскольку контролировать эту сеть невозможно, то необходима установка дополнительных паролей на последовательные порты.

Разграничение доступа пользователей к ресурсам (023)

Для разграничения доступа к файлам в ОС применяются наборы из трех флагов, разрешающих, соответственно, чтение, запись и выполнение файла. При этом каждый файл имеет пользователя-владельца, который и устанавливает перечисленные флаги для себя, членов своей группы и для прочих пользователей. Такой прием называется ***произвольным управлением доступом***, поскольку владелец действует по своему усмотрению.

По отношению к программам, переустанавливающим идентификатор пользователя, необходим контроль целостности и в плане прав доступа к программному файлу, и в плане его содержимого. Число таких программ желательно минимизировать и применять их только в крайнем случае.

Наличие нескольких путей получения повышенных привилегий является потенциально уязвимым местом в защите операционной системы. Особенно опасно, когда переустановка идентификатора пользователя производится не бинарным файлом, а программой командного интерпретатора, что объясняется легкостью ее модификации.

Указанное обстоятельство заставляет администратора системы контролировать штатные пользовательские командные интерпретаторы. Поскольку большинство пользователей обходится ограниченным набором приложений, в ряде случаев можно зафиксировать круг доступных программ, что особенно актуально при проведении нормативной политики безопасности. Свобода пользователя ограничивается пределами его каталога и возможностью использовать программы только из разрешенных каталогов.

Иногда пользователь вообще не нуждается в непосредственном взаимодействии с операционной системой, работая постоянно с каким-либо приложением, например клиентом базы данных. В этом случае целесообразно использовать возможности разграничения доступа, предоставляемые СУБД.

Средство проверки корректности конфигурации ОС (024)

Операционная система имеет большое количество настроек и конфигурационных файлов, что позволяет адаптировать ОС для нужд конкретных пользователей информационной системы. Однако это создает опасность появления слабых мест, поэтому для проверки целостности и корректности текущей конфигурации в ОС должна быть предусмотрена специальная утилита.

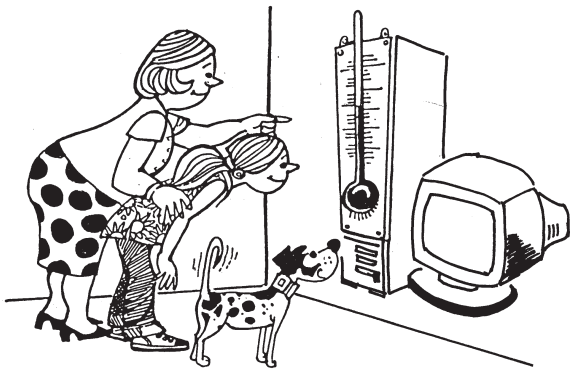
Данная утилита может быть настроена на один из трех уровней безопасности. На каждом последующем уровне доступ к ресурсам сокращается, делая систему более безопасной. На самом высоком уровне защиты ставится цель максимально ограничить возможности доступа в систему. При этом возможно изменение работы ряда системных сервисов.

При запуске утилита сначала проводит верификацию прав доступа к системным файлам. Затем проверяет системные файлы и сравнивает их с описанием в мастер-файле, который содержит установки, соответствующие избранному уровню безопасности. В ходе выполнения задачи для системных файлов проверяются владелец и группа, права доступа, размер и контрольная сумма, количество ссылок и время последней модификации.

Результаты выполнения программы записываются в текстовом виде в специальных файлах. Все корректировки, проводимые программой, протоколируются, и

систему можно в любой момент вернуть к прежнему состоянию, что страхует администратора от необратимых действий.

Инструмент системного аудита (720)



Инструмент системного аудита...

Вопросы информационной безопасности не могут успешно решаться, если нет средств контроля за происходящими событиями, поскольку только имея хронологическую запись всех производимых пользователями действий, можно оперативно выявлять случаи нарушения режима информационной безопасности, определять причины нарушения, а также находить и устранять потенциально слабые места в системе безопасности. Кроме того, наличие аудита в системе играет роль сдерживающего фактора: зная, что действия фиксируются, многие злоумышленники не рискуют совершать заведомо наказуемых действий.

Программные средства, осуществляющие такой контроль, называются средствами аудита. Поскольку в информационной системе предприятия имеется несколько функциональных уровней, на каждом из них желательны средства мониторинга событий. Сегодня наличие механизмов аудита является обязательным требованием к крупным программным продуктам, работающим на любом из уровней.

Аудит невозможен без идентификации и аутентификации пользователей. С этой целью при входе в систему программой аудита пользователю присваивается уникальный идентификатор, ассоциируемый с пользовательскими процессами, который остается неизменным, даже если пользователь с помощью команды su меняет свое имя. Регистрационные действия выполняются специализированным аудит-демоном, который проводит запись событий в регистрационный журнал в соответствии с текущей конфигурацией. Аудит-демон стартует в процессе загрузки системы.

Каждое событие принадлежит какому-либо классу аудита. Такое деление упрощает анализ большого количества событий. Принадлежность событий к классам и набор классов могут быть сконфигурированы системным администратором.

Существует около двадцати классов отслеживаемых событий. Каждый класс имеет два имени — полное и сокращенное. Для любого класса устанавливается один из трех флагов аудита: аудит в случае успешного выполнения действия, аудит неудачных попыток, безусловный аудит.

При работе модулей аудита на нескольких машинах их можно администрировать как части распределенной системы, когда каждая машина регистрирует события, а затем локальные регистрационные журналы собираются вместе, что позволяет анализировать все события, относящиеся к какому-либо классу или пользователю.

Сетевые средства защиты (024)

Защита информации на сетевом уровне имеет определенную специфику. Если на системном уровне проникнуть в систему можно было лишь в результате раскрытия пользовательского пароля, то в случае распределенной конфигурации становится возможен перехват пользовательских имени и пароля техническими средствами. Например, стандартный сетевой сервис telnet пересылает пользовательское имя и пароль в открытом виде. Это заставляет вновь рассматривать задачу аутентификации пользователей, но уже в распределенном случае, включая и аутентификацию машин-клиентов. Высокая степень защиты достигается путем замены стандартных открытых сервисов на сервисы, шифрующие параметры пользователя/машины-клиента, чтобы даже перехват пакетов не позволял раскрыть эти данные. Наконец, немаловажное значение имеет аудит событий, происходящих в распределенной информационной среде, поскольку в этих условиях злоумышленник не столь заметен и имеет достаточно времени и ресурсов для выполнения своих задач.

Стандартные средства защиты, существующие в ОС, не являются столь же объемлющими, что и на системном уровне. Дело в том, что если на системном уровне однородность гарантирована и любые изменения могут вводиться достаточно эффективно, то в условиях локальной сети применяется, как правило, набор разнородного оборудования, функционирующего под управлением различных ОС, производители которых априорно не заинтересованы в соответствии средств этих систем концепции безопасности.

Защита в сетевом информационном сервисе (024)

Сетевой информационный сервис (NIS) служит для централизованного управления информационными ресурсами в распределенной среде. Сервис работает на основе набора таблиц, содержащих сведения о машинах, параметрах удаленной загрузки, паролях, ключах аутентификации машин локальной сети, пользователях и группах, подсетях, сетевых масках, адресах Ethernet, сервисах, протоколах, параметрах автоматического монтирования удаленных файловых систем и удаленного вызова процедур (RPC). Поскольку указанная информация достаточно важна для безопасности информационной системы, ее надежная защита с учетом критериев конфиденциальности, целостности и доступности абсолютно необходима. Такая защита реализуется при использовании механизмов авторизации и аутентификации.

Права доступа в NIS определяют, какие операции доступны тому или иному клиенту. Операции подразделяются на четыре класса:

- чтение (Read),
- модификация (Modify),
- создание (Create),
- удаление (Destroy).

Каждое взаимодействие между клиентом и сервером может сводиться к запросу на проведение действий какого-либо из этих классов.

В NIS различаются четыре категории сетевых субъектов:

- владелец (Owner),
- группа владельца (Group),
- все (World),
- никто (Nobody),

В NIS имеется три уровня режима безопасности.

Уровень 0 используется для тестирования и установки начального набора имен. В этом режиме любому пользователю разрешен доступ к любому из объектов.

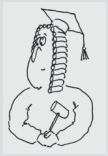
Уровень 1 применяется на стадии тестирования и отладки. При этом все механизмы авторизации работают в полной мере.

Уровень 2 используется, когда производится аутентификация клиентов с применением DES-ключей.

Kerberos-клиент [024]

Современные информационные системы, как правило, разнородны. Достаточно популярной является комбинация UNIX-серверов с рабочими местами на базе ПК с NT или MS-DOS. Количество сервисов, необходимых для каждого пользователя, может быть велико, причем некоторые сервисы могут требоваться неявно. Это делает актуальной задачу выделения аутентификации в сетевой конфигурации в особый сервис, с назначением сервера аутентификации.

Стандартом де-факто такого сервера является Kerberos, реализованный на коммерческих системах аутентификации как сетевого уровня (CygnusKerberos, OpenVSecure), так и уровня приложений (Tuxedo).



Определение

Система Kerberos представляет собой надежную третью сторону, которой доверяют все, владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности. В этом качестве Kerberos-сервер должен быть физически защищен и иметь минимальное количество пользователей, желательно — только системный администратор с локальной консоли.

Безопасность X-приложений (024)

Одна из особенностей современной операционной системы — возможность использования многооконного интерфейса для работы пользователей, для большинства UNIX-систем это стандарт X11. ***Поскольку X-сервер управляет такими ресурсами, как экран, клавиатура, «мышь», необходимо проводить разграничение доступа к этим ресурсам.*** При этом, с одной стороны, пользователь должен иметь возможность вызывать как локальные, так и удаленные X-приложения, в том числе выступая под различными пользовательскими именами, с другой стороны, несанкционированный доступ к этим ресурсам должен быть невозможен.

X-приложения...

Для решения этой задачи применяются различные варианты авторизации. Наиболее простой из них предполагает авторизацию по имени машины, запрашивающей сервис. Поскольку такой механизм авторизации заведомо недостаточен, разрешая работать своим удаленным приложениям, он неявно разрешает работу приложений всех других пользователей этой машины.

Доступность данных (020)

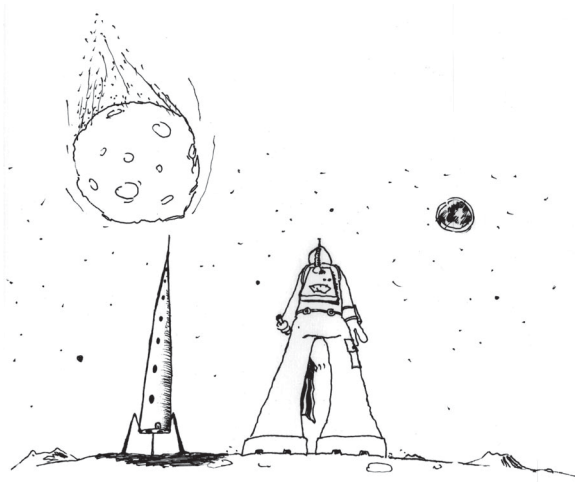
Компонент информационной безопасности — доступность — означает возможность получения необходимых пользователю данных или сервисов за разумное время. Однако существует вероятность сбоя в результате неправильных действий пользователя, аппаратной ошибки или иных причин. Это вынуждает обращаться к дополнительным средствам для увеличения надежности системы и, соответственно, доступности данных.

Средством повышения производительности и надежности дисковых систем является использование избыточных массивов RAID разных уровней. Для реализации технологии RAID создается псевдодрайвер, который помещается между пользовательскими приложениями и драйверами дисковых подсистем. Псевдодрайвер принимает пользовательские запросы на ввод/вывод и прозрачным для приложений образом переадресует их реальным устройствам. С точки зрения пользователя происходит увеличение скорости и надежности работы дисков без каких-либо аппаратных модификаций.

Увеличение надежности — одна из основных составляющих обеспечения доступности информационных ресурсов. Другой составляющей является систематическое ***резервное копирование программ и данных с целью минимизации ущерба при возможных сбоях.*** Эта задача становится достаточно сложной в условиях работы с распределенными ресурсами сети.

Целесообразно осуществлять централизованное создание резервных копий в рамках разнородной сети. При этом нобходимо обеспечить:

- возможность работы с клиентами под управлением большинства имеющихся ОС,
- графический интерфейс,
- встроенное протоколирование с извещением о возникающих проблемах,
- оповещение локальных клиентов о проведении резервного копирования,
- открытый программный интерфейс,
- поддержка широкого спектра устройств резервного копирования,
- возможность копирования не всей системы, а лишь ее части в соответствии с набором критериев.



Ядро безопасности...

Ядро безопасности ОС (020)

Ядро безопасности (ЯБ) ОС – набор программ, управляющих частями системы, ответственными за безопасность. ЯБ реализует политику обеспечения безопасности системы. Данная политика состоит из множества правил надзора и охраны взаимодействий между *субъектами* (процессы) и *объектами* (файлы, устройства, ресурсы межпроцессорного взаимодействия).

Определение

Действие в ОС ***подотчетно***, если его можно проследить для конкретного пользователя. ЯБ повышает подотчетность путем установления соответствия между всеми входами в систему и реальными пользователями.

ЯБ должно уникальным образом идентифицировать каждого пользователя. Для этого вводится еще один идентификатор пользователя — ***входной***. Это несмываемый штамп для каждого процесса, он не изменяется в течение всего сеанса работы.

Большинство ОС принимают решения о возможности доступа на основании простых прав доступа; процессы суперпользователя всегда получают доступ. ЯБ выделяет два типа полномочий: полномочия ядра и полномочия подсистем.

Полномочия ядра ассоциируются с процессами. Они позволяют процессу выполнить определенные действия, если процесс обладает необходимой привилегией.

Полномочия подсистем ассоциируются с пользователями. Они позволяют пользователю выполнять определенное действие посредством команд, отнесенных к подсистеме.

Подсистема — набор файлов, устройств и команд, служащих определенной цели. Полномочия ядра заносятся в «множество полномочий», ассоциированное с каждым процессом. Полномочия устанавливаются по умолчанию; пользователь может их и переустановить.

Когда пользователь входит в незащищенную ОС, имеет место ограниченная идентификация и проверка подлинности. Система по входному имени проверяет пароль в базе данных паролей. Если имя найдено, система опознает пользователя путем зашифрованного пароля с содержимым соответствующего поля в базе данных паролей.

ЯБ расширяет стандартный механизм. Существуют определенные правила, ограничивающие допустимые пароли, новые процедуры для генерации и изменения паролей. Расположение и защита определенных частей базы данных паролей изменены. Администратор имеет больший контроль над процессом входа. Этот аспект системы поддерживает отдельный пользователь — администратор опознавания.

Кроме того, ЯБ предоставляет полный «след» действий — ***журнал учета***. Журнал содержит записи о каждой попытке доступа субъекта к субъекту (успешные и неудачные), о каждом изменении субъекта, объекта, характеристик системы. Подсистема учета управляется специальным администратором учета. Администратор учета управляет собранной информацией, которая помогает администратору выяснить, что случилось с системой, когда и кто в этом участвовал.

Одна из важных функций ЯБ — локализация потенциальных проблем, связанных с безопасностью. Ограничительный механизм состоит из:

- парольных ограничений,
- ограничений на использование терминалов,
- входных ограничений.

Администратор опознавания может позволять пользователям самостоятельно вводить пароли или использовать сгенерированные пароли. Пароль может подвергаться проверке на очевидность.

Определяются следующие состояния паролей:

- пароль корректен,
- пароль просрочен (пользователь может войти в систему и изменить пароль, если у него есть на это полномочие,
- пароль закрыт (пользователь заблокирован; необходима помощь администратора).

Пользователи часто не подчиняются принудительной периодической смене паролей, восстанавливая предыдущее значение. Чтобы препятствовать этому, кроме максимального, устанавливается еще и минимальное время действия паролей.

Поддерживается возможность генерировать отчеты о различных аспектах функционирования системы: пароли, терминалы, входы.

Ни одна ОС не является абсолютно безопасной. Возможны следующие пути вторжения:

- некто может узнать пароль другого пользователя или получить доступ к терминалу, с которого в систему вошел другой пользователь;
- пользователь с полномочиями злоупотребляет своими привилегиями
- хорошо осведомленный пользователь получил неконтролируемый доступ непосредственно к компьютеру.

Как избежать подобных ситуаций?

Администратор должен следить за сменой паролей и запрещать входы в систему без паролей. Полезна также информация о неудачных попытках входа в систему.

Если есть причины подозревать лицо, имеющие полномочия суперпользователя в злоупотреблении привилегиями, следует включить для этого пользователя процедуру учета, чтобы определить, выполняет ли он подозрительные действия.

Опасно предоставлять оборудование для открытого доступа пользователям. Любые средства защиты системы будут бесполезны, если оборудование, носители сохраненных версий и дистрибутивы не защищены.

Подсистема учета ОС регистрирует происходящие в системе события, важные с точки зрения безопасности, в журнале учета, который впоследствии можно анализировать. Учет позволяет анализировать собранную информацию, выявляя способы доступа к *объектам* и действия конкретных пользователей. Подсистема учета с большой степенью надежности гарантирует, что попытки обойти механизм защиты и контроля полномочий будут учтены.

Сетевые серверы — это ворота, через которые внешний мир получает доступ к информации на Вашем компьютере. ***Поэтому ЯБ должно:***

- определить, какую информацию/действие запрашивает клиент;
- решить, имеет ли клиент право на информацию, которую запрашивает сервис;
- передать требуемую информацию/выполнить действие.

Ошибки в сервере и «черные ходы» могут подвергнуть опасности защиту всего компьютера, открывая систему любому пользователю в сети, осведомленному об изъяне. Даже относительно безобидная программа может привести к разрушению всей системы.

Виртуальные частные сети...

Технологии виртуальной частной сети для корпоративных пользователей (020)

Технология виртуальной частной сети (VPN) обеспечивает связь между сетями, а также между удаленным пользователем и корпоративной сетью с помощью защищенного канала (тоннеля), «проложенного» в общедоступной сети Internet. Данные, передаваемые по VPN, упаковываются в зашифрованные IP-пакеты. Владельцы VPN-сетей используют различные схемы шифрования и аутентификации, которые обеспечивают защиту данных.

VPN может быть развернута на базе Internet или построена на инфраструктуре других транспортных сетей: IP, Frame Relay или ATM. Основная масса решений по VPN разрабатывается для IP-сетей, наиболее известная из которых — Internet. Решения по VPN различных производителей разнообразны: от интегрированных многофункциональных и специализированных устройств до сугубо программных продуктов.

Существуют четыре основных протокола, используемых для создания VPN-сети: PPTP (Point-to-Point Tunneling Protocol — тоннельный протокол «точка-точка»), L2F (Layer 2 Forwarding — протокол продвижения пакетов на втором уровне), L2TP (Layer 2 Tunneling Protocol — тоннельный протокол второго уровня) и IPSec (IP Security Protocol — протокол, обеспечивающий шифрование пакетов протокола IP).

Экономические выгоды (020)

До появления VPN распределенные корпоративные сети преимущественно строились с использованием выделенных линий, а также технологий Frame Relay. Стоимость построения корпоративной сети на основе Internet с применением VPN-технологий значительно меньше стоимости создания сети на базе арендованных линий. Основные затраты при использовании VPN приходятся на оплату услуг Internet Service Provider и на расходы на VPN-оборудование. В условиях, когда число удаленных пользователей или офисов компании увеличивается, а стоимость аренды выделенных линий не снижается, применение технологии VPN становится особенно выгодным.

На рынке Internet-услуг число удаленных соединений, используемых для работы VPN, возрастает с каждым годом. Объясняется это феноменальным успехом системы Internet (как базы для корпоративных сетей), а также устойчивым увеличением количества мобильных и удаленных пользователей, использующих VPN-технологии. Удаленный доступ обеспечивает надежную и безопасную связь с корпоративной сетью через модемный пул Internet-провайдера.

Применение VPN-доступа уменьшит затраты на:

- закупку, монтаж и конфигурирование серверов удаленного доступа и модемов;
- сетевое оборудование;
- управление клиентским программным обеспечением;
- контроль трафика удаленного доступа;
- телефонные соединения;
- подготовку высококвалифицированных сетевых администраторов;
- изменение требуемого числа портов доступа при увеличивающемся количестве удаленных пользователей;
- линии связи.

Основные производители VPN-продуктов используют для обеспечения безопасности методы шифрования с 56-разрядным ключом, соответствующие стандарту DES. Такая длина ключа обеспечивает достаточно высокий уровень безопасности.

Однако для тех потенциальных покупателей, которые считают длину ключа в 56 бит небезопасной, некоторые поставщики VPN-продуктов предлагают шифрование по протоколу Triple DES. Тем не менее следует помнить, что слишком большое увеличение длины ключа снижает производительность, так как чем сложнее алгоритм шифрования, тем более интенсивной вычислительной обработки он требует.

Реализации технологий VPN (624)

Рынок VPN-продуктов в настоящее время развивается очень бурно. Потенциальным клиентам предлагается широкий спектр оборудования и ПО для создания VPN: от интегрированных многофункциональных и специализированных устройств до собственно программных продуктов.

Интегрированные VPN-решения включают функции межсетевого экрана, маршрутизации и коммутации. Главное преимущество такого подхода состоит в централизации управления компонентами. Специализированные VPN-системы обеспечивают более высокую производительность, так как шифрование в них осуществляется специализированными микросхемами. Чисто программные продукты обеспечивают производительность, достаточную для удаленного доступа.

Рассмотрим каждый вид VPN-решений:

1. ***Интегрированные VPN-решения***

Для компаний, которым не требуется высокая производительность корпоративной сети, а задача снижения расходов на сетевое оборудование является одной из приоритетных, наиболее эффективным будет интегрированное решение, позволяющее сосредоточить все функции в одном устройстве. При этом все же следует отметить, что чем больше функций исполняется одним устройством, тем чаще становятся заметными потери в производительности.

2. ***Специализированные VPN-решения***

Высокая производительность — главнейшее преимущество специализированных VPN-устройств. Объем вычислений, которые необходимо выполнить при обработке VPN-пакета, в 50-100 раз превышает тот, который требуется для обработки обычного пакета. Если в корпоративной сети проводятся различные мероприятия, требующие обмена большим трафиком данных, то для эффективной обработки VPN-пакетов необходимо использовать специализированную аппаратуру. Специализированные VPN-устройства обеспечивают высокий уровень безопасности.

3. ***Программные VPN-решения***

VPN-продукты, реализованные программным способом, с точки зрения производительности, конечно, уступают специализированным устройствам, однако обладают достаточной мощностью для реализации VPN-сетей. Следует отметить, что в случае удаленного доступа требования к необходимой полосе пропускания невелики. При создании модемного соединения даже у мобильного компьютера хватает вычислительной мощности, но все-таки программные реализации VPN не могут обеспечить работу на высоких скоростях каналов обмена данными.

Архитектура VPN-сетей (624)

В настоящее время существует несколько типов физических реализации VPN-технологий, каждая из которых характеризуется определенным набором функциональных требований.

Можно выделить три основных вида архитектуры применения VPN-продуктов:

- ***Intranet VPN*** — создание VPN-сетей между внутренними корпоративными отделами и удаленными филиалами;
- ***Remote Access VPN*** — создание VPN-сетей, объединяющих корпоративную сеть и удаленных или мобильных служащих;
- ***Extranet VPN*** — создание VPN-сетей, объединяющих корпорацию с ее стратегическими партнерами, клиентами и поставщиками. Intranet VPN обеспечивает создание безопасных соединений между внутренними отделами компании и ее филиалами.

Основные свойства Intranet VPN:

- применение мощных криптографических протоколов шифрования данных для защиты конфиденциальной информации;
- надежность функционирования при выполнении критических приложений, таких, как системы автоматизированной продажи и системы управления базами данных;
- гибкость управления для более эффективного размещения быстро возрастающего количества новых пользователей, новых офисов и новых программных приложений.

Архитектура Remote Access VPN обеспечивает функционирование корпоративной сети и удаленных (мобильных) пользователей.

Ее основные свойства:

- мощная система установления подлинности удаленных и мобильных пользователей, которая должна с максимальной точностью и эффективностью провести процедуру аутентификации;
- эффективная система централизованного управления для обеспечения высокой степени гибкости при увеличении количества пользователей, работающих с VPN.

Extranet VPN обеспечивает эффективное взаимодействие между корпорацией и ее стратегическими партнерами, клиентами и поставщиками. Для этого потребуются стандартизированные VPN-продукты, гарантирующие способность к взаимодействию с различными VPN-решениями, которые деловые партнеры могли бы применять в своих сетях.

Резюме

Необходимость защиты процессов, процедур и программ обработки данных от несанкционированного доступа и использования определяется следующими факторами:

- возможностью случайного или преднамеренного нарушения целостности и истинности вводимой или хранящейся информации на этапе ее ввода в ИС;
- возможностью нарушения целостности, истинности и сохранности информации при ее хранении;
- возможностью утечки, нарушения целостности, истинности и сохранности информации при ее обработке.
- возможностью утечки информации, при ее выводе для пользователя, который не должен иметь доступа к данной информации;
- возможностью утечки, нарушения целостности, истинности и сохранности информации при ее передаче между отдельными, территориально удаленными, ИС на жестких носителях или по линиям связи.

Широкомасштабное использование вычислительной техники и телекоммуникационных систем в рамках территориально распределенной сети, переход на этой основе к безбумажной технологии, увеличение объемов обрабатываемой информации, расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационной системы, к их высокой уязвимости.

Особенно остро стоит проблема обеспечения юридической значимости электронных документов, обработка которых осуществляется в информационных системах различного уровня.

В качестве наиболее приемлемого метода целесообразно использовать цифровую подпись электронных документов на основе несимметричного криптографического алгоритма, которая обеспечивает не только юридическую значимость, но также защиту целостности и аутентификацию документов.

Эффективность механизмов защиты информации в значительной степени зависит от реализации ряда принципов.

Во-первых, механизмы защиты должны проектироваться совместно с разработкой самой информационной системы, что позволяет обеспечить их бесконфликтность, своевременную интеграцию в вычислительную среду и сокращение затрат.

Во-вторых, вопросы защиты должны рассматриваться комплексно в рамках единой системы защиты информации (СЗИ) информационной системы. Системный подход обеспечивает адекватную многоуровневую защиту информации, рассматриваемую как комплекс организационно-правовых и технических мероприятий.

Ядро безопасности ОС (ЯБ) — набор программ, управляющих частями системы, ответственными за безопасность. ЯБ реализует политику обеспечения безопасности системы. Данная политика — это множество правил надзора и охраны взаимодействий между *субъектами* (процессы) и *объектами* (файлы, устройства, ресурсы межпроцессорного взаимодействия).

Действие в ОС *подотчетно*, если его можно проследить для конкретного пользователя. ЯБ повышает подотчетность путем установления соответствия между всеми входами в систему и реальными пользователями, учета каждого действия и сопоставления каждого действия конкретному пользователю.

ЯБ должно уникальным образом идентифицировать каждого пользователя. Для этого вводится еще один идентификатор пользователя — *входной*. Это несмываемый штамп для каждого процесса, он не изменяется в течение всего сеанса работы.

В настоящее время существует несколько типов физических реализации VPN-технологий, каждая из которых характиризуется определенным набором функциональных требований.

Можно выделить три основных вида архитектуры применения VPN-продуктов:

- Intranet VPN — создание VPN-сетей между внутренними корпоративными отделами и удаленными филиалами;
- Remote Access VPN — создание VPN-сетей, объединяющих корпоративную сеть и удаленных или мобильных служащих;
- Extranet VPN — создание VPN-сетей, объединяющих корпорацию с ее стратегическими партнерами, клиентами и поставщиками. Intranet VPN обеспечивает создание безопасных соединений между внутренними отделами компании и ее филиалами.

Основные свойства Intranet VPN:

- применение мощных криптографических протоколов шифрования данных для защиты конфиденциальной информации;
- надежность функционирования при выполнении критических приложений, таких, как системы автоматизированной продажи и системы управления базами данных;
- гибкость управления для более эффективного размещения быстро возрастающего количества новых пользователей, новых офисов и новых программных приложений.