Управление системой защиты

В этой главе

- *Принципы организации и контроля системы защиты*
- *Реализация политики безопасности*
- *Контроль за наиболее ценной информацией*
- *Административная группа управления защитой*
- *Опасные события и их предупреждение*
- *Идентификация, аутентификация и авторизация*
- *Методы разработки защищенных ИС*
- *Модели управления доступом*
- *Управление механизмами СЗИ*
- *Проблемы внедрения систем управления доступом*
- *Функции контроля и управление СЗИ*
- *Контроль за состоянием технической защиты информации*
- *Интеграция механизмов защиты ИС*

<<< 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

Управление защитой (050)

Управление защитой — это контроль за распределением информации в информационных системах. Он осуществляется для обеспечения функционирования средств и механизмов защиты; фиксации выполняемых функций и состояний механизмов защиты и фиксации событий, связанных с нарушением защиты (рис. 16.1 и 16.2).

Анализ сохранности СЗИ основывается на постоянном изучении протоколов (как машинных, так и ручных), проверке аварийных сигнализаторов и других устройств. Важным фактором является также и то, что такой обзор поддерживает интерес к вопросам обеспечения сохранности. За проведение анализа ответственность несет сотрудник, занимающийся вопросами обеспечения сохранности.

Приборы аварийной сигнализации следует проверять достаточно часто, но не в точно установленное время. К числу этих приборов относятся детекторы огня и дыма, датчики влажности и температуры, аппаратура сигнализации при попытках проникновения в помещение, устройства физического контроля доступа, дверная сигнализация и другие аналогичные приборы. Проводится также проверка состояния противопожарного оборудования, доступа к аварийным выходам и системам отключения электро-, водо- и теплоснабжения. Еженедельно проверяется исправность устройств и линий связи. Осматривается также пространство под технологическим полом и другие полости, в которых могут накапливаться отходы, создающие опасность самовозгорания, или вода при утечке. По проводимым работам ведется протокол проверки, каждая запись которого сопровождается замечаниями об отклонениях. Зарубежные специалисты считают, что для этой работы следует отводить около одного часа в неделю.

Кстати

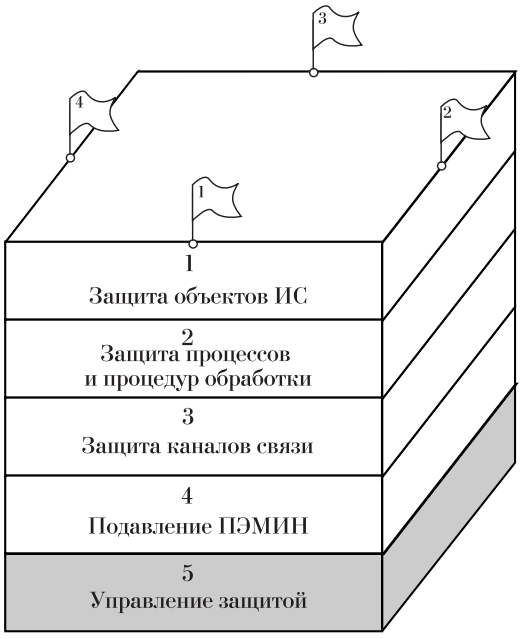


РИСУНОК 9.1. *Место вопросов управления защитой в общей структуре СЗИ.*

Рекомендуется тщательно исследовать любые подозрительные тенденции и отклонения от принятых стандартов в работе. Более того, описанные операции сами по себе являются объектом, сохранность которого необходимо обеспечить, поэтому должно быть выделено специальное помещение с терминалом, на котором выполняются только работы по обеспечению сохранности.

Побочным продуктом анализа сохранности может оказаться статистическая оценка эффективности использования ЭВМ и оценка эффективности работы пользователей. На основе результатов проверки проводятся еженедельные совещания, на которых заслушивается сообщение сотрудника, ответственного за обеспечение сохранности. Такие совещания позволяют оценить усилия по защите и выработать дополнительные рекомендации по совершенствованию принятых методов обеспечения сохранности.

Следует анализировать все возможности нарушения сохранности и отыскивать средства борьбы с ними. Если стандартные процедуры не выполняются, то повторяют инструктаж с целью выполнения этих процедур.

Кроме обычных регулярных проверок, описанных выше, сотрудник, ответственный за обеспечение сохранности, обязан выполнять тестовый контроль проверки аппаратуры и программного обеспечения. Результаты тестирования фиксируются в специальном журнале. Это требует некоторых затрат ручного труда и машинного времени. В информационных системах, где уровень обеспечения сохранности высок, тестирование должно проводиться более часто и по возможности автоматически. Результаты тестирования также анализируются сотрудником, ответственным за обеспечение сохранности.

Выбрать надежные средства защиты, отвечающие требованиям, это только полдела. Дальше необходимо настроить их так, чтобы все требования в части политики безопасности выполнялись так, как и было задумано (и зафиксировано в плане защиты). Кроме того, необходимо постоянно контролировать работу ИС.

Совет

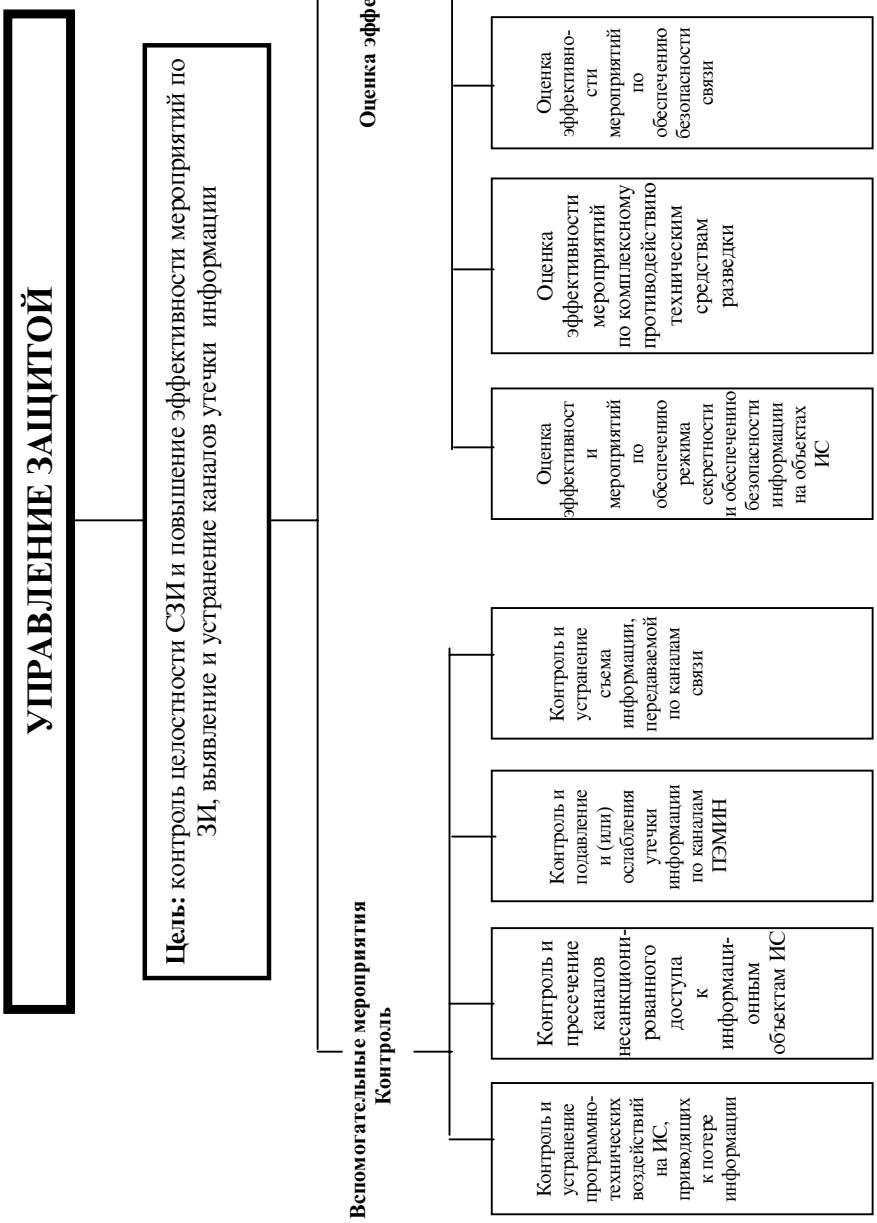


РИСУНОК 9.2. *Цель и задачи управления защитой.*

В принципе все это достаточно очевидно. Однако задачи настройки средств защиты, управления ими и контроля функционирования ИС в каждом конкретном случае решаются по-своему. Подходы к решению этих задач зависят от конкретных условий, поэтому приведем лишь основные положения, которыми следует руководствоваться при организации управления защитой ИС.

Если каждый пользователь работает автономно, решает только индивидуальные задачи и обрабатывает лишь собственные данные, то изоляция пользователей и индивидуальная защита позволят надежно оградить обрабатываемую информацию от различных угроз. Однако на практике такая ситуация встречается крайне редко. Почти всегда существует необходимость совместного решения различных задач или совместного анализа каких-либо данных, обмена информацией.

Это означает, что в системе существует информация, используемая несколькими пользователями. Это обстоятельство, в свою очередь, порождает проблему взаимного недоверия: если несколько пользователей имеют одинаковые права на какой-либо набор данных, то кто будет отвечать, если с ним что-либо случится?

Вообще, наличие любых совместно используемых ресурсов, тем более — доступных для модификации, создает предпосылки нарушения политики безопасности.

О том, как этого избежать, или хотя бы свести до минимума возможность нарушения политики безопасности либо, в крайнем случае, вовремя заметить и устранить последствия нарушения, пойдет речь далее.

Принципы организации и контроля системы защиты (750)

Настройка средств защиты, управление системой защиты и осуществление контроля функционирования ИС — все это составляющие одной задачи — реализации политики безопасности.

Управление средствами защиты включает в себя несколько задач, и их правильное решение способствует успешному функционированию ИС в целом. При этом, как правило, ни одна из крайностей — тотальная защита или полное ее отсутствие — не способствует оптимальной работе.

Кстати

Настройка средств защиты информации необходима для приведения их в соответствие с разработанным планом. При настройке добавленных средств защиты необходимо особое внимание уделить вопросам проверки их совместимости с используемыми прикладными программами.

Управление системой защиты состоит в периодическом внесении изменений в базу данных защиты, содержащую сведения о пользователях, допущенных к работе в системе, их правах доступа к различным объектам системы и др.

Особое внимание при управлении системой защиты необходимо обратить на:

- документированность всех изменений в базе данных защиты. Лучше всего организовать систему заявок от должностных лиц организации на разрешение доступа тому или иному сотруднику организации к какому-либо ресурсу системы. При этом ответственность за допуск сотрудника возлагается на соответствующее лицо, подписавшее заявку;
- периодическое резервное копирование базы данных защиты во избежание утраты их актуальной копии в случае сбоя (отказа) оборудования;

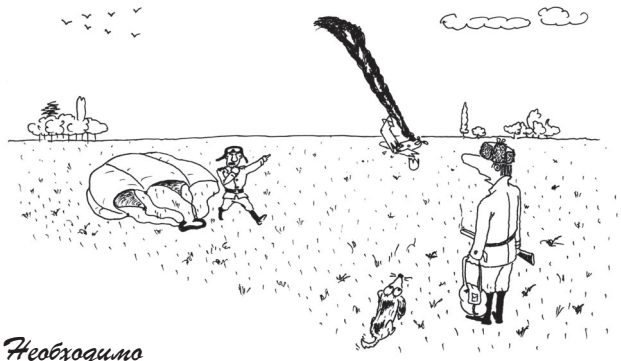
Контроль за функционированием ИС заключается в слежении за опасными событиями, анализе причин, которые привели к их возникновению, и устранении последствий.

Как правило, задачи управления и контроля решаются административной группой, личный и количественный состав которой зависит от конкретных условий. Обычно в эту группу входят: администратор безопасности, менеджер безопасности и операторы. Далее более подробно рассмотрим характеристики этой административной группы и функциональные обязанности входящих в нее сотрудников.

Обеспечение и контроль безопасности представляют собой комбинацию технических и административных мер. По данным, взятым из зарубежных источников, у сотрудников административной группы обычно 1/3 времени занимает техническая работа (управление программами и другими средствами контроля доступа, защита портов, криптозащита и т.д.) и около 2/3 — административная (разработка документов, связанных с защитой ИС, процедур проверки системы защиты, и т.д.). Рациональное сочетание этих мер помогает поддерживать адекватную защиту ИС и способствует уменьшению вероятности нарушений политики безопасности.

Администратор безопасности среднего и крупного банка на техническую работу тратит более 60% своего времени, а оставшиеся 40% уходят на решение административных задач. Это объясняется тем, что:

- количество сотрудников, входящих в административную группу, недостаточно для выполнения всех возложенных на группу обязанностей. Такое положение дел следует из недооценки руководящим составом организации роли и места обеспечения безопасности собственной ИС;



Необходимо координировать действия в рамках единой политики безопасности...

- производятся частые изменения программных средств, предназначенных для обработки информации (до 3–5 раз за одну неделю). Это связано с тем, что, как правило, крупные коммерческие банки содержат собственный штат программистов. А программисты находят и устраняют ошибки в программном обеспечении или дорабатывают программы в соответствии с требованиями аналитиков банка и затем обновляют программы;
- периодически изменяется штатно-должностное расписание (приходят новые сотрудники, уходят старые). Это приводит к тому, что иногда приходиться за неделю добавлять (удалять) в систему (из системы) 5–7 пользователей. Если система невелика — все не так сложно, а если ежедневно в ней работает одновременно более 100 человек с более чем 200 программными модулями, половина из которых обновляется, задача становится неимоверно тяжелой;
- отсутствуют программные средства, облегчающие деятельность администратора, поэтому администраторам приходится либо мириться с такой ситуацией, либо разрабатывать необходимые программные средства.

Реализация политики безопасности (053)

Политика безопасности и механизмы поддержки ее реализации образуют единую защищенную среду обработки информации. Эта среда имеет иерархическую структуру, где верхние уровни представлены требованиями политики безопасности, далее следует интерфейс пользователя, затем идут несколько программных уровней защиты (включая уровни ОС) и, наконец, нижний уровень этой структуры представлен аппаратными средствами защиты. На всех уровнях, кроме верхнего, должны быть реализованы требования политики безопасности, за что, собственно, и отвечают механизмы защиты.

В различных системах механизмы защиты могут быть реализованы по-разному; их конструкция определяется общей концепцией системы. Однако одно требование должно выполняться неукоснительно: эти механизмы должны адекватно реализовывать требования политики безопасности.

Совет

Меры по реализации и сопровождению политики безопасности в значительной степени зависят от конкретных условий, поэтому приведем лишь некоторые общие рекомендации (опуская анализ риска и составление плана защиты).

Оптимизация хранения и обработки информации (750)

Информацию в системе необходимо размещать таким образом, чтобы свести до минимума вероятность несанкционированного доступа. Это означает, что информацию, с одной стороны, следует организовать так, чтобы ее удобно было обрабатывать тем, кто должен с ней работать, а с другой, — чтобы к ней нельзя было получить доступ тем, кому это не разрешено.

Реализация принципов минимума привилегий и что “надо знать

Каждый пользователь должен иметь настолько мало привилегий, насколько это возможно без ущерба для работоспособности системы. Эти принципы — ключевые при определении полномочий пользователей и организации защиты наборов данных.

Разделение ответственности между пользователями

Каждый должен нести персональную ответственность за свои действия, при этом защиту следует организовать так, чтобы действия пользователей были как можно более независимыми. В тех случаях, когда это невозможно, и, следовательно, возникает проблема взаимного подозрения, следует использовать средства контроля.

Контроль за наиболее ценной информацией

Для предотвращения утечки или модификации наиболее ценной информации и для сохранения работоспособности ИС необходимо постоянное слежение за наиболее опасными событиями. Кроме того, необходимы регулярные проверки средств защиты и наиболее ценных объектов ИС.

Регулярный пересмотр положений политики безопасности и отражающих ее планов, используемых стандартов, своевременное внесение изменений, контроль за тем, чтобы средства защиты всегда были адекватны

требованиям политики безопасности. В частности, к этим мерам относится своевременное добавление и, особенно, удаление пользователей, отмена некоторых привилегий и т.д.

Взаимодействие с административными группами других ИС для координирования действий и проведения единой политики безопасности, затрагивающей общие аспекты обработки информации.

Это лишь самые общие рекомендации, справедливые практически для управления любой системой. Однако их точное соблюдение поможет сохранить работоспособность ИС в кризисных ситуациях, которые не так уж редки. Далее мы более подробно остановимся на мерах контроля за работой системы.

Для успешного решения основных задач административной группы, которые были перечислены, полезно учитывать следующие факторы:

Тип управления защитой

Управление может быть централизованным и децентрализованным. В зависимости от этого функциональные обязанности каждого сотрудника административной группы распространяются на всю систему или на какую-то ее часть.

Выбираемый тип управления целиком зависит от организационной структуры ИС и сложившейся технологии обработки информации.

Уверенность в безопасности

Администратор должен точно представлять себе все элементы защиты, степень уверенности пользователей в возможностях системы защиты, возможные угрозы системе и средства их предупреждения и т.д.

Возможности средств защиты

Для успешного решения задач управления защитой ИС административная группа должна использовать современные средства защиты, позволяющие гибко реагировать на все требования жизни.

Возможности администратора

Администратор безопасности — лицо в своем роде исключительное, должен быть представительным, респектабельным, иметь возможность взаимодействия с подразделениями и должностными лицами организации для более эффективного выполнения своих обязанностей.

Административная группа управления защитой (052)

Организация группы управления защитой информации, включающей специалистов в этой области — одна из наиболее важных задач управления защитой ИС. Иногда эту группу называют группой информационной безопасности.

Совет

В обязанности входящих в эту группу сотрудников должно быть включено не только исполнение директив вышестоящего руководства, но и участие в выработке решений по всем вопросам, связанным с процессом обработки информации с точки зрения обеспечения его защиты. Более того, все их распоряжения, касающиеся этой области, обязательны к исполнению сотрудниками всех уровней и организационных звеньев. Кроме того, организационно эта группа должна быть обособлена от всех отделов или групп, занимающихся управлением самой системой, программированием и другими относящимися к системе задачами во избежание возможного столкновения интересов.

Несмотря на то, что обязанности и ответственность сотрудников группы информационной безопасности варьируются в разных учреждениях, можно выделить несколько основных положений, которым должны соответствовать функциональные обязанности во всех организациях.

В обязанности сотрудников группы информационной безопасности входит:

Управление доступом пользователей системы к данным, включая установку и периодическую смену паролей, управление средствами защиты коммуникаций и криптозащиту передаваемых, хранимых и обрабатываемых данных.

Разработка планов защиты и контроль за их соблюдением, а также контроль за хранением резервных копий.

Доведение до пользователей изменений в области защиты, которые имеют к ним отношение, обучение персонала и пользователей ИС.

Взаимодействие со службой менеджмента ИС по вопросам защиты информации.

Совместная работа с представителями других организаций по вопросам безопасности — непосредственный контакт или консультации с партнерами или клиентами.

Тесное сотрудничество и дружественные отношения со службой менеджмента и администрацией ИС.

Расследование причин нарушений защиты.

Координация действий с аудиторской службой, совместное проведение проверок.

Постоянная проверка соответствия принятых в организации правил безопасности обработки информации существующим правовым нормам, контроль за соблюдением этого соответствия.

Поддержание хороших отношений с теми отделами, чьи задачи могут (по каким-то особым причинам) выполняться в обход существующих правил.

Естественно, все эти задачи не под силу одному человеку, особенно если организация (компания, банк и др.) довольно велика. Более того, ***в группу управления защитой могут входить сотрудники с разными функциональными обязанностями. Обычно выделяют четыре группы сотрудников (по возрастанию иерархии):***

1. **Сотрудник группы безопасности**
В его обязанности входит обеспечение должного контроля за защитой наборов данных и программ, помощь пользователям, организация общей поддержки групп управления защитой и менеджмента в своей зоне ответственности. При децентрализованном управлении каждая подсистема ИС имеет своего сотрудника группы безопасности.

2. **Администратор безопасности системы**
В его обязанности входит ежемесячное опубликование нововведений в области защиты (новых стандартов), контроль за выполнением планов непрерывной работы, восстановление системы после сбоев, хранение резервных копий.

3. **Администратор безопасности данных**
В его обязанности входит реализация и изменение средств защиты данных, контроль за состоянием защиты наборов данных, ужесточение защиты в случае необходимости, а также координирование работы с другими администраторами.

4. **Руководитель (начальник) группы** по управлению обработкой информации и защитой
В его обязанности входит разработка и поддержка эффективных мер защиты при обработке информации для обеспечения сохранности данных, оборудования и программного обеспечения; контроль за выполнением плана восстановления и общее руководство административными группами в подсистемах ИС (при децентрализованном управлении).

Существует несколько вариантов детально разработанного штатного расписания такой группы, в которые включен перечень функциональных обязанностей, необходимых знаний и навыков, распределение времени и усилий. При организации защиты существование такой группы и детально разработанные обязанности ее сотрудников совершенно необходимы.

Опасные события и их предупреждение (250)

Для того, чтобы предотвратить угрозу безопасности или устранить ее последствия, прежде всего необходимо ясно представлять, какие вообще возможны угрозы ИС. Для большинства ИС перечень угроз, которые могут повлечь за собой частичную или полную потерю информации или работоспособности системы и которые будем называть опасными, один и тот же. К ним можно отнести:

1. Перехват информации из линии связи.

2. Перехват паролей.

3. Попытка проникновения в систему.

4. Создание или изменение записей базы данных защиты.

5. Несанкционированное получение и использование привилегий.

6. Несанкционированный доступ к наборам данных.

7. Установка непроверенных выполняемых модулей и командных процедур, где могут таиться “Троянские кони”, “черви” и т.д.

8. “Сборка мусора” на диске или в оперативной памяти.

9. Использование узлов сети как портов для проникновения в другие узлы сети ЭВМ.

В каждом из этих случаев должны предприниматься немедленные меры для предотвращения нарушения работоспособности ИС и сохранения данных.

При этом необходимо остановиться на таком опасном нарушении, как несанкционированный доступ (НСД). Дело в том, что понятие “несанкционированный” достаточно трудно определить.

Чаще всего под НСД понимают проникновение пользователя к информации, которая ему не должна быть доступна. Это возможно в двух случаях:

1. В программно-аппаратных средствах поддержки политики безопасности есть ошибки, приводящие к возможности действий, позволяющих их обход. В этом случае единственный выход — смена средств защиты (внести исправления в рабочем порядке обычно не представляется возможным).

2. Когда НСД оказался возможен в результате некорректно сформулированной или реализованной политики безопасности для данной конфигурации технических и программных средств системы.

Для исключения случаев НСД следует пересмотреть политику безопасности или способы ее реализации, проверить полноту и однозначность сформулированных требований. Этот вопрос больше относится к проектированию и реализации средств защиты или политики безопасности, но никак не к управлению защитой.

По мнению специалистов фирмы «Информ-защита», для того, чтобы корректно воплотить в жизнь разработанную политику безопасности необходимо иметь надежные механизмы ее реализации.

Кстати

Естественно предположить, что все средства, ответственные за реализацию политики безопасности, сами должны быть защищены от любого вмешательства в их работу. В противном случае говорить о надежности защиты будет трудно. Можно изменять их параметры, но в своей основе они должны оставаться в неприкосновенности.

Все средства защиты и управления должны быть объединены в так называемую достоверную вычислительную базу. **Достоверная вычислительная база (ДВБ)** — это абстрактное понятие, обозначающее полностью защищенный механизм вычислительной системы (включая аппаратные и программные средства), отвечающий за поддержку реализации политики безопасности.

Средства защиты должны создавать ДВБ для обеспечения надежной защиты ИС. В различных средствах защиты ДВБ может быть реализована по-разному. Способность реализации ДВБ к безотказной работе зависит от ее устройства и корректного управления, а ее надежность является залогом соблюдения политики безопасности в защищаемой системе.

Таким образом, ДВБ выполняет двойную задачу — поддерживает реализацию политики безопасности и является гарантом целостности механизмов защиты, т.е. самой себя. ДВБ совместно используется всеми пользователями ИС, однако ее модификация разрешена только пользователям со специальными полномочиями. К ним относятся администраторы системы и другие привилегированные сотрудники организации.

Процесс, функционирующий от имени ДВБ, достоверен. Это означает, что система защиты безоговорочно доверяет этому процессу и все его действия санкционированы политикой безопасности. Именно поэтому задача номер один защиты ДВБ — поддержание собственной целостности; все программы и наборы данных ДВБ должны быть надежно защищены от несанкционированных изменений.

Для поддержки политики безопасности и собственной защиты ДВБ должна обеспечить защиту субъектов (процессов) системы и защиту объектов системы в оперативной памяти и на внешних носителях.

Защита ДВБ строится на основе концепции иерархической декомпозиции системы.

Особенность применения концепции иерархической декомпозиции заключается в следующем:

1. Каждый компонент должен выполнять строго определенную функцию;

2. Каждая функция с помощью операции декомпозиции может быть разбита на ряд подфункций, которые реализуются и защищаются отдельно. Этот процесс может насчитывать несколько этапов;

3. Основная “тяжесть” защиты приходится на межуровневый интерфейс, связывающий декомпозированные подфункции в единое целое; горизонтальные ссылки должны быть сведены до минимума.

Помимо защиты самой себя ДВБ также должна обеспечить надежную защиту пользователей системы (в частности, друг от друга). Для защиты пользователей используются те же механизмы, что и для защиты ДВБ. Неизменны и цели защиты: субъектов и объектов пользователей, в оперативной памяти и на внешних носителях.

Доступ к информации на внешних носителях осуществляется с помощью подсистемы ввода/вывода; программы этой подсистемы являются компонентами нижних и средних уровней ДВБ. При получении имени файла (адреса записи) в первую очередь проверяются полномочия пользователя на доступ к запрашиваемым данным. Решение на осуществление доступа принимается на основе информации, хранящейся в базе данных защиты. Сама база данных представляет собой часть ДВБ, доступ к которой также контролируется.

Одним из необходимых условий реализации ДВБ в средствах защиты является наличие мультирежимного процессора (т.е. процессора, имеющего привилегированный и обычный режимы работы) с аппаратной поддержкой механизма переключения режимов и различных способов реализации виртуальной памяти.

Достоверная вычислительная база состоит из ряда механизмов защиты, позволяющих ей обеспечивать поддержку реализации политики безопасности.

Основой ДВБ является **ядро безопасности** — элементы аппаратного и программного обеспечения, защищенные от модификации и проверенные на корректность, которые разделяют все попытки доступа субъектов к объектам.

Ядро безопасности представляет собой реализацию концепции монитора ссылок (reference monitor) — абстрактной концепции механизма защиты.

Помимо ядра безопасности ДВБ содержит другие механизмы, отвечающие за жизнедеятельность системы. К ним относятся планировщики процессов, диспетчеры памяти, программы обработки прерываний, примитивы ввода/вывода и другие программно-аппаратные средства, а также системные наборы данных.

Определение

Под монитором ссылок понимают концепцию контроля доступа субъектов к объектам в абстрактной машине.

Под базой данных защиты понимают базу данных, хранящую информацию о правах доступа субъектов системы к объектам. Основу базы данных защиты составляет матрица доступа (МД) или ее представления, которая служит основой избирательной политики безопасности.

Любая операционная система, поддерживающая избирательное управление доступом (ИУД), использует МД и операции над ней, поскольку МД — удобный инструмент контроля использования и передачи привилегий.

Монитор ссылок должен выполнять следующие функции:

1. Проверять права доступа каждого субъекта к любому объекту на основании информации, содержащейся в базе данных защиты и положений политики безопасности (избирательной или полномочной);

2. При необходимости регистрировать факт доступа и его параметры в системном журнале.

Реализующее монитор ссылок ядро безопасности должно соответствовать следующим требованиям:

- контролировать все попытки доступа субъектов к объектам;
- иметь защиту от модификации, подделки, навязывания;
- быть протестировано и верифицировано для получения гарантий надежности;
- иметь небольшой размер и компактную структуру.

Идентификация, аутентификация и авторизация (054)

Эти функции необходимы для подтверждения подлинности субъекта, законности его прав на данный объект или на определенные действия, а также для обеспечения работы субъекта в системе.

Идентификация — процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой априорной информации; каждый субъект или объект должен быть однозначно идентифицируем.

Аутентификация — проверка идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа); а также проверка целостности данных при их хранении или передаче для предотвращения несанкционированной модификации.

Авторизация — предоставление субъекту прав на доступ к объекту.

При входе в систему и вводе имени пользователя осуществляется идентификация, при вводе пароля — аутентификация, и если пользователь с данными именем и паролем зарегистрирован в системе, ему разрешается доступ к определенным объектам и ресурсам (авторизация).

Как показывает практика, вход пользователя в систему — одно из наиболее уязвимых мест защиты; известно множество случаев взлома пароля, входа без пароля, его перехвата и т.д. Поэтому при выполнении входа и пользователь, и система должны быть уверены, что они работают непосредственно друг с другом, между ними нет других программ и вводимая информация истинна.

Достоверный маршрут реализуется привилегированными процедурами ядра безопасности, работа которого обеспечивается механизмами ДВБ, а также некоторыми другими механизмами, выполняющими вспомогательные функции.

Регистрация и протоколирование (054)

Эти функции обеспечивают получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля, а также регистрацию действий, признанных администрацией потенциально опасными для системы.

Надежными считаются биометрические методы аутентификации по голосу...

Такими средствами могут быть различные системные утилиты или прикладные программы, выводящие информацию непосредственно на системную консоль или другое определенное для этой цели устройство, а также системный журнал. Кроме того, почти все эти средства контроля могут не только обнаружить какое-либо событие, но и фиксировать его.

Например, большинство систем имеет средства протоколирования сеансов работы отдельных пользователей (всего сеанса или его отдельных параметров).

Большинство систем защиты имеют в своем распоряжении ***средства управления системным журналом (audit trail)***. Это — одно из основных средств контроля, помогающее администратору предотвращать нарушения в благодаря способности:

- оперативно фиксировать происходящие в системе события;
- выявлять средства и априорную информацию, использованные злоумышленником для нарушения;
- определять степень нарушения, подсказывать метод его расследования и способы исправления ситуации.

Содержимое системного журнала и других наборов данных, хранящих информацию о результатах контроля, должны подвергаться периодическому пересмотру и анализу (аудит) с целью проверки соблюдения политики безопасности.

Противодействие "сборке мусора"

По окончании работы программы обрабатываемая информация не всегда полностью удаляется из памяти. Части данных могут оставаться в оперативной памяти, на дисках и лентах, других носителях. Они хранятся на диске до перезаписи или уничтожения. При выполнении этих действий на освободившемся пространстве диска находятся их остатки.

Хотя при искажении заголовка файла эти остатки прочитать трудно, однако используя специальные программы и оборудование, такая возможность все-таки имеется. Этот процесс называется "сборкой мусора" (disk scavenging) Он может привести к утечке важной информации.

Для защиты от "сборки мусора" используются специальные средства, которые могут входить в ядро безопасности ОС или устанавливаться дополнительно.

Контроль целостности

Контроль целостности обеспечивается процедурами ядра безопасности, контролируемыми механизмами поддержки ДВБ. Основную роль играют такие механизмы, как поддержка виртуальной памяти (для создания области данного процесса) и режим исполнения процесса (определяет его возможности в рамках данной области и вне ее).

Область исполнения процесса может содержать или вкладываться в другие подобласти, которые составляют единую иерархическую структуру системы. Процесс может менять области, что называется переключением области процесса (process switching). Оно всегда связано с переходом центрального процессора в привилегированный режим работы.

Контроль доступа

Под контролем доступа будем понимать ограничение возможностей использования ресурсов системы программами, процессами или другими системами (для сети) в соответствии с политикой безопасности. Под доступом понимается выполнение некоторой операции над объектом из множества разрешенных для данного типа. Примеры таких операций — чтение, открытие, запись набора данных, обращение к устройству и т.д.

Контроль должен осуществляться при доступе к:

- оперативной памяти;
- устройствам прямого доступа;
- устройствам последовательного доступа;
- программам и подпрограммам;
- наборам данных.

Основным объектом внимания средств контроля доступа являются совместно используемые наборы данных и ресурсы системы. Совместное использование объектов порождает ситуацию "взаимного недоверия", при которой разные пользователи одного объекта не могут до конца доверять друг другу. Тогда, если с этим объектом что-нибудь случится, все они попадают в круг подозреваемых.

Существует четыре основных способа разделения субъектов к совместно используемым объектам:

- **физическое** — субъекты обращаются к физически различным объектам (однотипным устройствам, наборам данных на разных носителях и т.д.);
- **временное** — субъекты с различными правами доступа к объекту получают его в разное время;
- **логическое** — субъекты получают доступ к совместно используемому объекту в рамках единой операционной среды, но под контролем средств разграничения доступа, которые моделируют виртуальную операционную среду "один субъект — все объекты";
- **криптографическое** — все объекты хранятся в зашифрованном виде, права доступа определяются наличием ключа для расшифрования объекта.

Существует множество вариантов одних и тех же способов разделения субъектов, они могут иметь разную реализацию в различных средствах защиты.

Группирование

Это объединение множества субъектов под одним групповым именем; всем субъектам, принадлежащим к одной группе, предоставляются равные права. Принципы объединения пользователей в группы могут быть самые разные: ссылки на одни и те же объекты, одинаковый характер вычислений, работа над совместным проектом и т.д. При этом один и тот же субъект может входить в несколько групп, и, соответственно, иметь различные права по отношению к одному и тому же объекту.

Механизм группирования может быть иерархическим. Это означает, что каждый субъект является членом нескольких групп, упорядоченных по отношению "быть подмножеством". Контроль за состоянием необходим, поскольку члены одной группы имеют доступ к большому числу объектов, что не способствует усилению их безопасности. Создание групп и присвоение групповых привилегий должно производиться администратором безопасности, руководителем группы или каким-либо другим лицом, ответственным за сохранность групповых объектов.

Правила умолчания

При назначении привилегий следует уделять внимание правилам умолчания, принятым в данных средствах защиты; это необходимо для соблюдения политики безопасности. Во многих системах, например, субъект, создавший объект и являющийся его владельцем, по умолчанию получает все права на него. Кроме того, он может эти права передавать.

В различных средствах защиты используются свои правила умолчания, однако принципы назначения привилегий по умолчанию в большинстве систем одни и те же. Если в системе используется древовидная файловая структура, то необходимо принимать во внимание правила умолчания для каталогов. Корректное использование правил умолчания способствуют поддержанию целостности политики безопасности.

Минимум привилегий

Это один из основополагающих принципов реализации любой политики безопасности, используемый повсеместно. Каждый пользователь и процесс должны иметь минимальное число привилегий, достаточное для работы. Определение числа привилегий для всех пользователей, с одной стороны, позволяющих осуществлять быстрый доступ ко всем необходимым для работы объектам, а с другой, — запрещающих доступ к чужим объектам — проблема достаточно сложная. От ее решения во многом зависит корректность реализации политики безопасности.

Объединение критичной информации

Во многих системах сбор, хранение и обработка информации одного уровня производится в одном месте (узле сети, устройстве, каталоге). Это объясняется тем, что проще защитить одним и тем же способом большой массив информации, чем организовывать индивидуальную защиту для каждого набора.

Для реализации этого принципа могут быть разработаны специальные программы, управляющие обработкой таких наборов данных. Это — простейший способ построения защищенных областей.

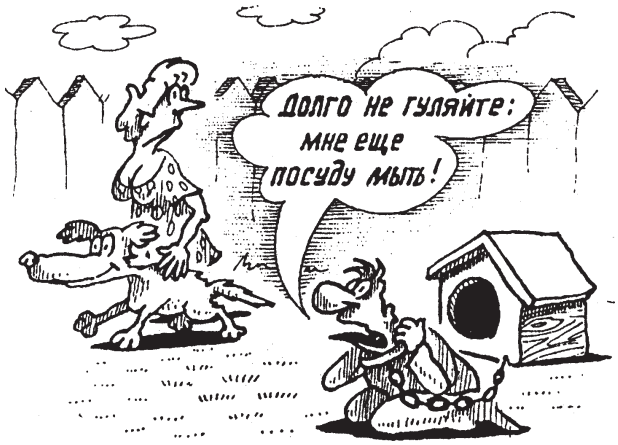
Иерархия привилегий

Контроль объектов системы может иметь иерархическую организацию. Такая организация принята в большинстве коммерческих систем. При этом схема контроля имеет вид дерева, в котором узлы — субъекты системы, ребра — право контроля привилегий, согласно иерархии, корень — администратор системы, имеющий право изменять привилегии любого пользователя.

Достоинство такой структуры — точное копирование схемы организации, которую обслуживает ИС. Поэтому легко составить множество субъектов, имеющих право контролировать данный объект. Недостаток иерархии привилегий — сложность управления доступом при большом количестве субъектов и объектов, а также возможность получения доступа администратора системы (как высшего по иерархии) к любому набору данных.

Привилегии владельца

При таком контроле каждому объекту соответствует единственный субъект с исключительным правом контроля объекта — владелец (owner). Как правило, это его создатель. Владелец обладает всеми разрешенными для



Минимум привилегий...

этого типа данных правами на объект, может разрешать доступ любому другому субъекту, но не имеет права кому-либо передать привилегию на корректировку защиты. Однако такое ограничение не касается администраторов системы — они имеют право изменять защиту любых объектов.

Главным недостатком принципа привилегий владельца является то, что при обращении к объекту, пользователь должен предварительно получить разрешение у владельца (или администратора). Это может привести к сложностям в работе (например, в отсутствие владельца или при его нежелании разрешить доступ). Поэтому такой принцип обычно используется при защите личных объектов пользователей.

Свободная передача привилегий

При такой схеме субъект, создавший объект, может передать любые права на него любому другому субъекту вместе с правом корректировки этого объекта. Тот, в свою очередь, может передать все эти права другому субъекту.

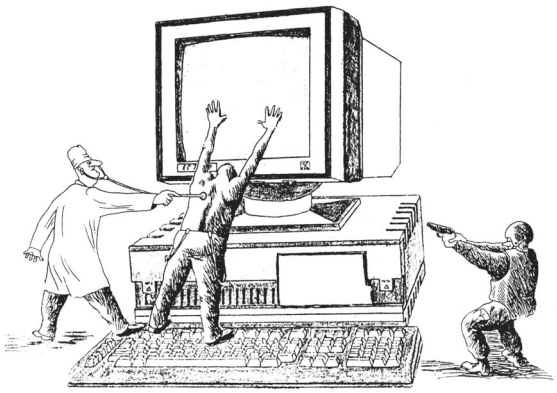
Естественно, при этом возникают трудности в определении круга субъектов, имеющих в данный момент доступ к объекту (права на объект могут быстро распространяться и так же быстро исчезать); поэтому такой объект легко подвергается несанкционированной обработке.

В чистом виде рассмотренные принципы реализации политики безопасности применяются редко. Обычно используются их комбинации. Ограничение доступа к объектам в ОС включает в себя ограничение доступа к некоторым системным возможностям, например ряду команд, программам и другим средствам, если при использовании их нарушается политика безопасности.

Вообще набор полномочий каждого пользователя должен быть тщательно продуман, должны быть исключены возможные противоречия и дублирование, поскольку многие нарушения происходят именно по этим причинам. Не исключена утечка информации и без нарушения защиты, если плохо спроектирована или реализована политика безопасности.

Предотвращение угроз информации (650)

НСД может быть обнаружен с помощью средств контроля или явиться побочным эффектом другого нарушения (например, вирусной атаки), но причины его гораздо глубже. Во всяком случае говорить о возможности НСД можно только в том случае, если строго определено понятие “несанкционированный”.



НСД может быть обнаружен с помощью средств контроля...

Когда систему пытаются атаковать, умышленно или неумышленно, информацию об этом можно получить из следующих источников:

- от пользователей — о состоянии защиты личных наборов данных отдельных пользователей;
- при мониторинге функционирования ИС — о состоянии общих характеристик системы;
- из системного журнала — о состоянии защиты различных наборов данных.

Рассмотрим подробнее, как на основе информации каждого из перечисленных источников распознать угрозу.

Пользователи (052)

В случае, когда средства защиты функционируют некорректно, пользователи обязаны известить об этом администратора защиты. Это могут быть следующие ситуации:

- потеря набора данных или ошибки при обращении к нему;
- неудовлетворительное содержание сообщения о последнем входе (зафиксирован более поздний вход в систему, чем в действительности);
- неудача при входе в систему — возможно, изменен пароль;
- зафиксирована попытка проникновения и, как следствие, невозможность входа в систему;
- наличие наборов данных, которые никогда не создавались;
- неожиданные изменения защиты личных объектов пользователя;

- появление листингов, сообщений и другой информации под именем пользователя, который их не генерировал;
- истощение ресурсов пользователя (например, памяти на диске).

Каждая возникающая ситуация нуждается в тщательном анализе, результаты которого должны быть известны соответствующим пользователям.

Мониторинг функционирования ИС (750)

Под мониторингом системы подразумевается получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля. Такими средствами могут быть различные системные утилиты или прикладные программы, выводящие информацию непосредственно на системную консоль или другое определенное для этой цели устройство. Отличительная особенность мониторинга — получение и анализ информации, осуществляемые в реальном времени.

Приведем перечень ситуаций возможного нарушения защиты, информацию о которых можно получить с помощью мониторинга:

- в списке пользователей упомянуты такие, которые не должны в настоящее время работать в системе;
- неожиданные события при загрузке системы;
- нарушения физической защиты — неработоспособны или утеряны носители информации;
- изменения в списке пользователей, допущенных к защищенным файлам;
- появление в системных библиотеках выполняемых модулей, которые не были проверены;
- обнаружение выполнения неизвестных программ при контроле системы;
- добавление неизвестных имен к списку привилегированных пользователей;
- во время сеанса работы пользователей зафиксировано чрезмерно большое время использования процессора — возможно, вследствие НСД;
- в очереди пакетных заданий находятся неизвестные или подозрительные;
- в ИС обнаружены неизвестные устройства;
- наблюдается повышенный уровень загруженности системы;
- неожиданное изменение характеристик системы (средств) защиты;
- изменение характера работы пользователей.

Этот список может быть дополнен еще множеством других ситуаций. Для каждой ИС такой список индивидуален. Здесь приведены лишь наиболее часто встречающиеся ситуации, которые могут сигнализировать об угрозе. Появление каждой из них должно быть тщательно и своевременно проанализировано во избежание потенциальной опасности.

Кроме того, средства контроля, как правило, фиксируют сведения о прошедшем событии. Например, большинство систем имеет средства протоколирования сеансов работы отдельных пользователей. ***Отчеты об этом помогут обнаружить:***

- неизвестные имена пользователей;
- настораживающие характеристики сеансов — неурочные часы или дни работы, например чрезмерное использование ресурсов системы; источники некорректных входов в систему, узлы сети, удаленные терминалы и др.

Системный журнал (054)

Для того, чтобы своевременно выявлять и предотвращать опасные события, необходим системный журнал. Работа с ним — частный случай мониторинга функционирования ИС, однако его обычно считают самостоятельным средством контроля. Дело в принципиальном различии их целей: в процессе мониторинга осуществляется слежение за общими характеристиками системы и он осуществляется оператором, а системный журнал регистрирует состояние средств защиты и управляется администратором безопасности.

По ряду причин системный журнал представляет собой одно из основных средств контроля, способствующее предотвращению возможных нарушений.

В журнале оперативно фиксируются происходящие в системе события, например:

- вводимые команды и имена выполняемых программ,
- доступ к определенным наборам данных или устройствам и его параметры,
- вход/выход пользователей из системы,
- имя терминала или другого устройства, с которого был осуществлен ввод команды или запуск программы,
- случались ли похожие события ранее и кто (что) был их причиной,
- другие события;

Анализ содержимого системного журнала может помочь выявить средства и априорную информацию, использованные злоумышленником для осуществления нарушения. Ведь очевидно, что без предварительной информации любая сознательная попытка нарушения

почти наверняка обречена на провал. К такой информации можно отнести:

- данные об ИС,
- сведения о структуре организации,
- знание параметров входа в систему (имена и пароли),
- информация об используемом оборудовании и программном обеспечении,
- характеристики сеансов работы и т.д.

Кроме того, анализ содержимого системного журнала может помочь определить, как далеко зашло нарушение, подсказать метод его расследования и способы исправления ситуации.

Естественно, с помощью одного системного журнала не всегда удается определить источник нарушения, однако он несомненно позволяет значительно сузить круг подозреваемых.

В дополнение к перечисленным мерам ***рекомендуется обязательный контроль следующих событий с помощью системного журнала:***

1. События типа “ошибка входа” или “попытка проникновения” (если “ошибка входа” фиксируется слишком часто — больше трех раз подряд). Это лучший способ распознавания попыток проникновения в систему.

2. События типа “вход в систему”. Помогает контролировать работу, особенно при доступе к узлу из сети. Такой доступ является источником повышенной опасности.

3. События типа “ошибка при доступе к набору данных”. Дает возможность обнаружить попытки преодоления защиты наиболее ценных объектов ИС.

4. Запись (доступ типа WRITE) в наборы данных. Помогает предотвратить их несанкционированную модификацию. При этом необходимо учитывать особенности модификации некоторых системных наборов.

5. Осуществление действий, на которые необходимы различного рода привилегии. Дает возможность выявить злоупотребления ими.

Мониторинг функционирования системы и системный журнал дают умелому администратору мощное средство слежения за функционированием системы. Однако изобилие информации, поступающее в результате мониторинга и анализа системного журнала, может быть эффективно обработано лишь при наличии у администратора специальных средств работы с этой информацией.

Устранение нарушений (750)

Используя информацию, поступающую от пользователей, на основе мониторинга и записей системного журнала, оператор системы должен своевременно обнаруживать нарушения и предпринимать меры по их локализации и устранению. Если его знаний или полномочий недостаточно, такую работу выполняет администратор безопасности.

В случае установления попытки или факта проникновения в систему администратор безопасности или оператор обязан предпринять следующие меры:

- локализовать нарушение,
- установить личность нарушителя,
- предотвратить дальнейшие нарушения,
- попытаться устранить последствия нарушения.

Прежде всего, необходимо локализовать нарушение, т.е. установить, кто нарушитель, каковы его действия и дальнейшие намерения. Для этого следует определить круг подозреваемых: кто мог это сделать? Кто имел необходимые полномочия? Кто умел это делать? Затем, используя имеющуюся информацию, сужать этот круг. Так, определив, с какого терминала осуществлено нарушение, в какое время и каким образом, вы значительно сузите круг подозреваемых.

Конкретные действия оператора и/или администратора безопасности в каждом случае определяются особенностями ИС и системы защиты. Каждая попытка нарушения может оказаться удачной или неудачной. В зависимости от этого должны предприниматься соответствующие действия. Далее рассмотрим эти этапы более подробно.

Неудачные попытки проникновения (052)

Под неудачными попытками проникновения понимают безуспешные попытки угадать или перехватить пароль, а также попытки НСД.

Они обычно обнаруживаются, если:

- пользователи сообщают о неожиданных ошибках входа;
- установлены необычные действия в системе или использование недействительных коммутируемых линий;
- система вывела тревожные сообщения об ошибках входа, попытках проникновения, нарушениях защиты наборов данных;
- обнаружены записи об опасных событиях в системном журнале.

Определение нарушителя (252)

Установить личность нарушителя очень просто с помощью соответствующего вида контроля, если он является пользователем данного узла сети. В этом случае имя нарушителя фиксируется в системном журнале вместе с характеристиками нарушения. Далее следуют организационные выводы.

Установить личность нарушителя очень просто...

Если нарушитель является пользователем другого узла сети, свои действия необходимо согласовывать с администратором защиты этого узла. Дело в том, что системный журнал данного узла может зафиксировать только точку входа в систему и характеристики входа. Так, если проникновение произошло с удаленного узла, то системный журнал зафиксирует только его имя. С помощью другой информации можно проследить вход в лучшем случае до соседнего узла, т.е. установить имя его пользователя, осуществившего вход на данный узел.

Установление нарушителя, осуществившего проникновение издалека с помощью сети, задача сложная и порой неразрешимая. Даже если удастся определить имя нарушителя, то, во-первых, сложно установить, кто скрывается за ним, а во-вторых, наказать его. Последняя задача иногда вообще нереальна. Он может находиться в другой организации, другом городе или за границей. Такие методы применяются лишь в самых крайних случаях, поскольку требуют много времени (до месяца и более), труда, привлечения дополнительных специалистов и, следовательно, денежных средств.

Всегда предпочтительнее использовать превентивные меры, чем потом тратить время и деньги на поиск нарушителя (а поиск может и не увенчаться успехом). Единственный надежный способ избежать этих сложностей — установить контроль за проникновением в ИС и постараться не допускать его.

Предотвращение попыток проникновения подразумевает действия относительно потенциальных нарушителей и прогнозирует возможное усложнение таких попыток. ***Чтобы свести до минимума вероятность успешного перехвата паролей, необходимо:***

1. Разрешить определенным пользователям выбор подходящего пароля. Предупреждать их о возможности перехвата пароля. Использовать генератор паролей.

2. Использовать для входа пароль администратора. Это лучший способ защиты от проникновения, доставляющий лишь небольшие дополнительные неудобства пользователям. Если системный пароль уже разрешен, изменить его.

3. Провести анализ успешных входов в систему для определения возможных проникновений.

Пароль не нужен (252)

Самая большая проблема для администраторов сетей — собственный персонал. Никто не желает возиться с паролями только потому, что администрация фирмы решила засекретить свою информацию. Пароли вешают на стенку, выписывают на клавиатуре, кладут под стекло. Но даже если персонал достаточно осторожен, поставщики секретного оборудования могут свести на нет все потуги администрации на полную конфиденциальность.

Для уменьшения вероятности успешного НСД необходимо:

1. По возможности установить нарушителя, немедленно предпринять соответствующие действия, предусмотренные для данной ИС планом защиты.

2. Предупредить пользователей о необходимости адекватной защиты наборов данных; регулярно проверять защиту наиболее ценных из них.

3. Если сетевой НСД становится периодическим, резко ограничить возможный доступ из сети или запретить его.

В случае установления факта неудачной попытки проникновения никаких действий по ликвидации последствий предпринимать не требуется, за исключением блокировки повторных нарушений подобного рода.

Удачные попытки проникновения (252)

Такие попытки подразумевают успешный захват пароля, ознакомление с информацией или ее искажение, истощение системных ресурсов, разрушение программного обеспечения. Они требуют много времени для ликвидации последствий в зависимости от квалификации и возможностей нарушителя.

Определение личности нарушителя — наиболее трудный этап при ликвидации последствий проникновения. Прежде всего, необходимо установить, является ли нарушитель зарегистрированным пользователем системы. Это может определить порядок дальнейших действий.

Пример

Хакер по кличке Хесс из Ганновера открыл телефонный справочник и выяснил номер телефона, по которому можно связаться с компьютером лаборатории в Беркли. Он соединился с ним через модем, и жутко засекреченная сеть потребовала пароль. Хесс недолго думал, набрав GUEST. Система пропустила его дальше (!) и перед самым входом в базу данных потребовала дополнительный пароль. Хесс угадал его со второй попытки. Дополнительный пароль был таков: VISITOR. Трудно догадаться, верно?

Именно Хесс с присущей ему наглостью первым пролез в базу данных Пентагона – сеть OPTIMI. Для входа потребовалось два слова: ANONYMOUS и GUEST. Взломав таким образом секретную сеть, Хесс получил доступ к 29 документам по ядерному оружию, в том числе, например, к такому: "План армии США в области защиты от ядерного, химического и бактериологического оружия".

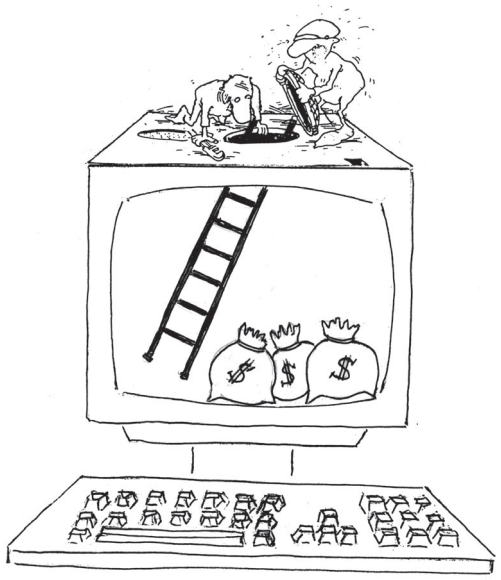
Затем этот любознательный юноша пролез через Беркли в компьютер космического отделения ВВС США в Лос-Анджелесе, создал счет на свое имя и произвел себя в полковники. Попался он глупо – ему подсунули базу данных Минэнерго США, переименовав ее файлы так, чтобы они напоминали документы СОИ. Хесс обалдел от счастья и слишком долго висел на линии, разбираясь в документах, так что его проследили до самой квартиры.

Но Хесса выловило отнюдь не ЦРУ, а обычный программист по имени Клиффорд Столл. Он сообщил о взломщике в ЦРУ, причем тут же разгорелся нешуточный скандал – фирма MITRE, отвечающая за безопасность указанных сетей, заявила, что сломать ее сети невозможно. Тогда Столл созвал журналистов и публично влез в ее сеть. Пароль для входа в сеть MITRE был, разумеется, MITRE!

Информация, полученная в результате контроля, зачастую бывает неполной. В таких случаях можно разрешить дальнейшее проникновение, если необходимо получить о нем более полную информацию. Тогда в соответствующих системных процедурах, находящихся под полным контролем администратора, организуются "люки" для получения дополнительной информации.

Следует позаботиться о восстановлении наборов по резервным копиям в случае их уничтожения или модификации. Наиболее сложно определить нарушителя при проникновении через сеть, особенно при использовании коммутируемых (или выделенных) линий связи. Связанные с этим трудности мы рассмотрели ранее.

Меры, которые необходимо предпринять после установления факта проникновения, зависят от его сущности. Основные перечислены ниже в порядке возрастания предполагаемого ущерба:



Организуются "люки" для получения информации...

1. Обезопасить базу данных защиты (хранящую информацию о пользователях и их полномочиях, а также о защите объектов системы).

2. Изменить пароли, если есть подозрения в их компрометации. Изменить хотя бы пароли привилегированных пользователей, строго следя за тем, чтобы они не повторялись для разных пользователей.

3. Полностью или частично обновить системные модули из резервных копий.

4. Ужесточить защиту. Применить дополнительные меры по защите наборов данных; использовать системные пароли, генераторы паролей; усилить меры контроля.

Первоочередной мерой по ликвидации последствий проникновения в систему должна быть перезагрузка модифицированных или уничтоженных файлов. Следует также определить, обязательна ли полная перезагрузка данных; пересмотреть защиту файлов; выяснить, имелась ли возможность при данном нарушении внести в системные или прикладные модули "червей", "троянских коней" и пр.

В случае положительного решения произвести уничтожение и перезагрузку соответствующих компонентов системы. Разумное сочетание этих мер поможет избежать многих опасностей — уж где-нибудь злоумышленник да проявит себя; важно не упустить его.

Дополнительные меры контроля (753)

Случается, что обычных мер контроля, предлагаемых системой, может оказаться недостаточно. Тогда ***применяют специально разработанные дополнительные меры. К ним можно отнести, во-первых, статистические меры контроля.*** Особые программы постоянно следят за состоянием некоторых параметров системы, постоянно отслеживая их изменение. Специальная экспертная система периодически (в определенные моменты или при изменении определенных параметров) анализирует состояние контролируемых параметров, при этом, возможно, сравнивая их с предыдущими значениями (на основе методов многомерного статистического анализа). При появлении каких-либо отклонений сразу выдается тревожное сообщение. Это своего рода автоматизация мониторинга системы. Такие методы уже достаточно хорошо разработаны, некоторые из них реализованы.

Во-вторых, к дополнительным мерам можно отнести некоторые интеллектуальные средства. Если ИС имеет большие размеры, следить за состоянием ее защиты трудно. Поэтому можно установить специальные программные средства, которые будут настроены на анализ определенных состояний системы, например на опасные события или изменение конфигурации. Они могут вовремя сообщить о появлении возможности НСД или каналов утечки информации, которые обычным способом обнаружить трудно.

Пример

Примером средств контроля, совмещающего черты как статистических, так и интеллектуальных средств, может быть контроль банковских операций. С помощью такого контроля можно автоматически следить за пересылаемыми суммами, номерами счетов, местом назначения, временем платежа. Если какой-то отдельный параметр или их комбинация перейдут в разряд запрещенных (например, размер платежа превышает установленный), подается сигнал тревоги. Эта же система может накапливать и анализировать определенные сведения в течение длительного периода. Так, она может контролировать все переводы на определенный счет, и, если за определенный промежуток времени сумма превысит допустимую, также выдается сигнал тревоги. Можно назвать еще множество полезных функций, которые могла бы выполнять такая система.

Управление защитой в распределенных сетях (750)

Какой бы ни была защита системы распределенных вычислений, она (защита) нуждается в повседневном управлении: регистрации новых пользователей, исключении уволившихся сотрудников, изменении прав и привилегий при изменении характера деятельности работника.

Управление безопасностью в распределенных системах становится особенно сложным. Основная трудность заключается в том, что в ситуации, когда имеются распределенные системы и распределенная же информация, каждое подразделение несет ответственность только за свою платформу. Так, главной ЭВМ управляет одна группа работников, ЛВС — другая. Если ЛВС несколько, то ими могут управлять различные люди.

В большинстве случаев ответственность за информационную безопасность возлагается не на специально выделенное подразделение, а на подразделения пользователей, в которых администратор ЛВС одновременно выполняет и функции администратора информационной безопасности.

Не менее размыта ответственность и в сфере безопасности линий связи. Когда-то все связи исходили из единого центра, откуда они могли легко контролироваться квалифицированными специалистами, Сегодня управление сместилось вниз, в сторону отдельных корпораций. В связи с этим в настоящее время проблема информационной безопасности, по мнению специалистов, представляется скорее организационной, нежели технической.

Бесспорно, различные системы нуждаются в различной жесткости защиты. ЛВС, предназначенная для рутинного текстового редактирования и поддержки электронных таблиц, может быть защищена значительно слабее, чем производственная система с циркулирующей по ней важной внутрифирменной информацией.

Управление информационными потоками (050)

Чтобы получить информацию о каком-либо объекте ИС, вовсе не обязательно искать пути несанкционированного доступа к нему. Можно получать информацию, наблюдая за работой системы и, в частности, за обработкой интересующего объекта. Иными словами, при помощи каналов утечки информации.

По этим каналам можно получать информацию не только о содержимом объекта, но и о его состоянии, атрибутах и других параметрах в зависимости от особенностей системы и установленной защиты объектов. Эта особенность объясняется тем, что при взаимодействии субъекта и объекта возникает некоторый поток информации от субъекта к объекту (информационный поток)

Информационные потоки существуют в системе всегда. Поэтому возникает необходимость определить, какие из них в системе — “легальные”, т.е. не ведут к

утечке информации, а какие — ведут. Таким образом, возникает необходимость разработки правил, регулирующих управление информационными потоками в системе.

Для этого необходимо построить модель системы, которая может описывать такие потоки. Такая модель разработана Гогеном и Мисгаером (Goguen Meseguer model) и называется потоковой.

Надо знать

Модель описывает условия и свойства взаимного влияния (интерференции) субъектов, а также количество информации, полученной субъектом в результате интерференции. Управление информационными потоками в системе не есть самостоятельная политика, так как оно не определяет правил обработки информации. Оно применяется обычно в рамках избирательной или полномочной политики, дополняя их и повышая надежность системы защиты. В рамках полномочной политики оно является основой требований к классу B2 стандарта "Оранжевая книга"

Избирательное и полномочное управление доступом, а также управление информационными потоками — своего рода три кита, на которых строится вся защита.

Управление надежностью (050)

Важным фактором обеспечения защиты информации является контроль работы оборудования и программного обеспечения. При этом следует обращать внимание как на исходный контроль оборудования и программ до момента их эксплуатации, так и на последующие периодические проверки качества функционирования. В период между проверками должен быть организован строгий контроль за изменениями в оборудовании и программах. Должны быть предусмотрены специальные стандартные процедуры контроля оборудования и программ после их модификации.

В случае использования общих каналов связи для передачи сообщений и обмена информацией надежность работы линий связи значительно снижается. Однако помехоустойчивое защитное кодирование с высоким уровнем рабочего фактора может повысить надежность линий связи.

Управление доступом (050)

Управление доступом (избирательное или полномочное) сравнительно легко реализуемо (аппаратно или программно), однако оно неадекватно реальным ИС из-за существования в них скрытых каналов. Тем не менее управление доступом обеспечивает достаточно надежную защиту в простых системах, не обрабатывающих особо важную информацию. В противном случае средства защиты должны дополнительно реализовывать управление информационными потоками.

Организация управления доступом...

Организация такого управления в полном объеме достаточно сложна, поэтому его обычно используют для усиления надежности полномочной политики: восходящие (относительно уровней безопасности) информационные потоки считаются разрешенными, все остальные — запрещенными.

Отметим, что, кроме способа управления доступом, политика безопасности выдвигает еще и другие требования, такие, как подотчетность, гарантии и т.д.

Эти процедуры сводятся к взаимному опознанию пользователя и системы и установлению факта допустимости использования ресурсов конкретным пользователем в соответствии с его запросом. Кроме того, управление доступом разрешает обслуживание системой запроса пользователя и получение доступа к файлам данных. Средства управления доступом обеспечивают защиту информации как от неавтоматизированного использования, так и от несанкционированного обслуживания системой. Защита реализуется процедурами идентификации, установления подлинности и регистрации обращений.

Если система предоставляет средство управления доступом, то коды идентификации пользователя, пароли и другая информация обеспечения безопасности хранятся в таблице авторизации. Последняя может находиться в защищенной зоне основной памяти или храниться как файл данных на дополнительном устройстве. Каждый авторизованный пользователь имеет свою запись в таблице авторизации.

Другой способ проверки подлинности пользователя — диалог по методу "запрос-ответ". Пользователь должен ответить правильно на вопросы, задаваемые

операционной системой из списка, хранящегося в памяти ЭВМ. В зависимости от степени важности глубина и продолжительность диалога различны. Возможна также передача операционной системой управления служебной программе пользователя для проведения диалога.

Идентификация и подтверждение подлинности могут осуществляться в процессе работы неоднократно, чтобы исключить возможность входа в систему нарушителя, выдающего себя за истинного пользователя. Запросы на идентификацию и подтверждение подлинности формулируются системными программами.

Во всех случаях положительной проверки подлинности пользователь получает право работать с системой. При отрицательной проверке вся необходимая информация регистрируется, и вводится временная задержка ответов на запросы этого пользователя с целью исключения раскрытия механизма защиты методом проб и ошибок.

После установления подлинности пользователя, в соответствии с запросом, проверяются его полномочия. Для выполнения этих действий система защиты должна иметь информацию по каждому пользователю, терминалу или другому ресурсу о допустимых процедурах со стороны запрашивающего. Все попытки входа в систему (как удачные, так и отвергнутые) должны регистрироваться в системном журнале с целью воссоздания при необходимости ретроспективы обращений к пользователю, терминалу, файлу, программе или любому другому ресурсу. По установленной периодичности пользователям для проверки направляются выписки из системного журнала, что позволяет следить за попытками нарушения сохранности защищаемых ресурсов и принимать необходимые меры при наличии угроз.

Методы разработки защищенных ИС (051)

Известно, что при разработке современных информационных систем используется один из двух методов:

Нисходящий метод (“сверху-вниз”): сначала составляется общее описание системы; выделяются компоненты системы; поэтапно увеличивается степень детализации компонентов системы (выделение компонентов в компонентах и т.д.) — до момента окончания разработки.

Восходящий метод (“снизу-вверх”): сначала формулируются задачи системы; затем разрабатывается некоторый набор элементарных функций; на базе элементарных функций разрабатываются более крупные компоненты системы — и так поэтапно разработка ведется до момента объединения отдельных компонентов в единую систему.

Наибольшее распространение получил компромиссный вариант, при котором разработка системы в целом ведется нисходящим методом, а разработка отдельных компонентов системы (в основном элементарных) — восходящим.

Особый интерес представляет нисходящий метод создания систем, так как этот метод позволяет задавать требования безопасности ко всей системе в целом и затем их детализировать применительно к каждой подсистеме.

Метод неформальной разработки применяется при создании относительно простых систем с небольшим числом компонентов и очевидными алгоритмами их взаимодействия.

По мере усложнения системы, взаимосвязи ее компонентов становятся все менее очевидными; сложно описать эти взаимосвязи с достаточной степенью точности неким неформальным образом (например, на естественном языке). При разработке систем обеспечения безопасности точность в описании компонентов и их взаимосвязей — едва ли не решающее условие достижения успеха, поэтому для обеспечения надлежащей степени точности применяется строгий аппарат формальной математики, что и составляет суть формального метода разработки.

Модели управления доступом (051)

Основную роль в методе формальной разработки системы играет так называемая ***модель управления доступом***. В англоязычной литературе для обозначения сходного понятия используются термины “security model” (модель безопасности) и “security policy model” (модель политики безопасности).

Эта модель определяет правила управления доступом к информации, потоки информации, разрешенные в системе таким образом, чтобы система всегда была безопасной.

Целью модели управления доступом является выражение сути требований по безопасности к данной системе. Для этого ***модель должна обладать несколькими свойствами:***

- быть адекватной моделируемой системе и неизбыточной;
- быть простой и абстрактной, и поэтому несложной для понимания.

Модель позволяет провести анализ свойств системы, но не ограничивает реализацию тех или иных механизмов защиты. Поскольку модель — формальна, возможно осуществить доказательство различных свойств безопасности всей системы.

Моделирование требует значительных усилий и дает хорошие результаты только при наличии времени и

ресурсов. Если система уже создана и имеется возможность сделать лишь отдельные изменения в отдельных местах существующей системы ("залатать дыры"), моделирование будет непродуктивным занятием.

На сегодня создан ряд типовых моделей управления доступом, которые можно использовать при разработке системы.

Все подобные модели, рассматривающие доступ субъекта к объекту, можно назвать ***моделями управления доступом***.

Модель конечного автомата описывает систему как абстрактную математическую машину. В этой модели переменные состояния представляют состояния машины, а функции перехода описывают способ изменения переменных. Модель управления доступом работает только с наиболее существенными переменными состояния, влияющими на безопасность, и потому намного проще, чем полная модель конечного автомата для данной системы.

Модель матрицы доступа это частный случай реализации модели машины состояний. Состояния безопасности системы представлены в таблице, содержащей по одной строке для каждого субъекта системы и по одной колонке для каждого субъекта и объекта. Каждое пересечение в массиве определяет режим доступа данного субъекта к каждому объекту. Второй составляющей модели матрицы доступа является набор функций перехода, описывающих способ изменения матрицы доступа.

Чаще матрица доступа используется не как самостоятельная модель управления доступом, а в качестве одной из нескольких переменных состояния в более общей модели конечного автомата.

Модель меток безопасности выраженная в терминах, приписываемых субъектам и объектам системы. В этом случае режим доступа, которым располагает субъект по отношению к объекту, определяется при сравнении их меток безопасности. Модель может использовать как матрицу доступа, так и атрибуты безопасности.

Модель информационных потоков предназначена для анализа потоков информации из одного объекта в другой на основании их меток безопасности

Модель интерференции, в которой субъекты, работающие в различных доменах, защищены от влияния друг на друга любым способом, нарушающим свойства безопасности системы.

Модель — лишь формулировка в математических терминах свойств безопасности, которым должна удовлетворять система. Не существует формального способа, с помощью которого можно доказать, что формальная модель управления доступа соответствует правилам управления доступа, принятым в данной системе.

С другой стороны, модель может иметь ряд характеристик, назначение которых не столь очевидно. Поскольку модель должна стремиться к математическому совершенству (завершенности и последовательности) в определении свойств, составляющих политику безопасности, это часто влечет за собой включение ограничений или дополнительных свойств, присутствие которых ранее не предусматривалось.

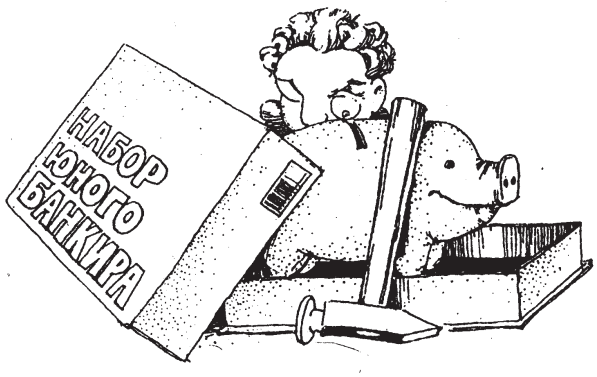
Разработка модели управления доступом предусматривает определение элементов модели (переменных, функций, правил и т.д.), а также безопасного начального состояния. Математически доказывается, что начальное состояние безопасно и что все функции безопасны, после чего делается вывод о том, что, если система первоначально находилась в безопасном состоянии, она останется в безопасном состоянии независимо от того, какие функции и в каком порядке будут выполнены.

Итак, в ***разработке модели управления доступом можно выделить следующие шаги:***

1. ***Определение переменных состояния, имеющих отношение к безопасности***. Обычно переменные состояния представляют субъекты и объекты системы, их атрибуты безопасности и права доступа между субъектами и объектами.

2. ***Определение условий для безопасного состояния***. Это определение представляет собой выражение отношений между значениями переменных состояния, истинность которого должна обеспечиваться при переходах состояния.

3. ***Определение функций переходов из состояния в состояние.*** Эти функции описывают допустимые способы изменения переменных состояния. Они также называются правилами изменения доступа, поскольку их цель состоит в указании изменений, которые может производить система, а вовсе не в определении всех возможных изменений. Правила могут быть очень об-



Модель управления доступом...

щими и могут допускать наличие функций, которых нет в реальной системе, однако система не может менять переменные состояния каким-либо способом, который не допускается функциями.

4. ***Доказывается, что функции обеспечивают сохранение безопасного состояния***. Чтобы удостовериться в том, что модель безопасна, необходимо для каждой функции перехода доказать, что, если система находится в безопасном состоянии до начала выполнения функции перехода, то она останется в таком состоянии по ее завершении.

5. ***Определение начального состояния.*** Математически начальное состояние выражается как множество начальных значений всех переменных состояния системы. Простейшим начальным состоянием является состояние вообще без каких-либо субъектов и объектов. При этом нет необходимости определять начальные значения каких-либо других переменных состояния, поскольку состояние будет безопасным независимо от их значений. Более реалистичное безопасное начальное состояние предполагает наличие некоторого начального (произвольного) множества субъектов и объектов.

6. ***Доказывается, что начальное состояние безопасно по определению.***

Помимо выполнения основной своей задачи — математически точного представления требований правил управления доступом, модель управления доступом используется в процессе разработки системы для выполнения так называемого анализа информационного потока.

Анализ информационного потока — это общая технология для анализа путей утечки информации в системе, она применима к любой модели безопасности.

Информационный поток может рассматриваться как отношение причина — следствие между двумя переменными A и B. Считается, что в любой функции, где модифицируется B и упоминается A, существует поток от переменной A к переменной B (записывается в виде A->B), если какая-либо информация о старом значении A может быть получена путем анализа нового значения B.

Модель управления доступом плохо пригодна для выявления таких слабостей в безопасности, как скрытые каналы, которые по сути являются незапланированными (и в большинстве — незаконными) информационными потоками. Вполне возможна ситуация, когда модель управления доступом, безупречная с точки зрения определений и доказательств, может содержать множество скрытых каналов, благодаря которым все усилия по реализации установленной политики безопасности теряют смысл.

Скрытые каналы достаточно эффективно выявляются в процессе анализа информационного потока, для которого основой может служить модель безопасности.

На практике анализ потока редко выполняется для системы на уровне абстрактной модели. Хотя анализ потока в модели может, конечно, выявить многие потенциальные нарушения потока, он может также и упустить ряд таких нарушений. Это возможно потому, что модель оставляет вне рассмотрения многие детали системы, например такие, как переменные состояния и функции, которые не влияют на безопасное состояние системы и, по определению, не включаются в состав модели безопасности. Именно эти внутренние переменные состояния обеспечивают возможность возникновения скрытых каналов.

С другой стороны, анализ информационного потока, выполненный на уровне модели системы, дает возможность выявить и устранить нежелательные скрытые каналы до того, как разработчики приступят к выполнению последующих шагов формального метода разработки системы.

Разработка и доказательство модели управления доступом системы — важный этап в формальном методе разработки системы. Сам формальный метод разработки можно ограничить этапом формального моделирования, после которого следует практическая реализация системы.

Управление механизмами СЗИ (754)

Достижения в области разработки средств защиты компьютерных систем привели к унификации перечня общих требований к этим средствам. Одним из пунктов в таком унифицированном списке практически всегда можно встретить требование наличия средств управления всеми имеющимися защитными механизмами.

Определение

Разработчики систем защиты основное внимание уделяют реализации самих защитных механизмов, а не средств управления ими. Такое положение дел свидетельствует о незнании или непонимании и недооценке проектировщиками и разработчиками большого числа психологических и технических препятствий, возникающих при внедрении разработанных систем защиты. Успешно преодолеть эти препятствия можно только, обеспечив необходимую гибкость управления средствами защиты.

Недостаточное внимание к проблемам и пожеланиям заказчиков, к обеспечению удобства работы администраторов безопасности по управлению средствами защиты на всех этапах жизненного цикла компьютерных систем часто является основной причиной отказа от использования конкретных средств защиты.

Проблемы внедрения систем управления доступом (650)

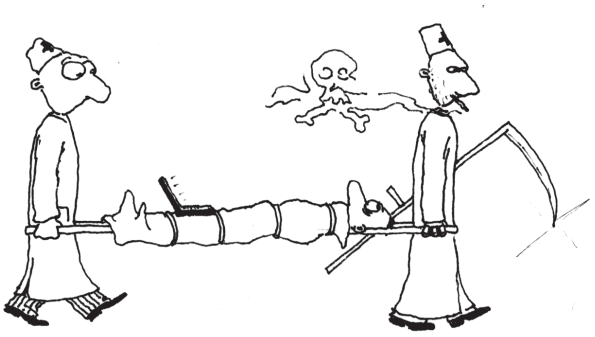
Опыт внедрения и сопровождения систем разграничения доступа в различных организациях позволяет указать на ряд типовых проблем, возникающих при установке, вводе в строй и эксплуатации средств разграничения доступа к ресурсам компьютерных систем, а также предложить подходы к решению этих проблем.

В настоящее время в большинстве случаев установка средств защиты осуществляется на уже реально функционирующие ИС заказчика.

Защищаемая ИС используется для решения важных прикладных задач, часто в непрерывном технологическом цикле, и ее владельцы и пользователи крайне негативно относятся к любому, даже кратковременному, перерыву в ее функционировании для установки и настройки средств защиты или частичной потере работоспособности ИС вследствие некорректной работы средств защиты.

Внедрение средств защиты усложняется еще и тем, что правильно настроить данные средства с первого раза обычно не представляется возможным. Это, как правило, связано с отсутствием у заказчика полного детального списка всех подлежащих защите аппаратных, программных и информационных ресурсов системы и готового непротиворечивого перечня прав и полномочий каждого пользователя ИС по доступу к ресурсам системы.

Поэтому, этап внедрения средств защиты информации обязательно в той или иной мере включает действия по первоначальному выявлению, итеративному уточнению и соответствующему изменению настроек средств защиты. Эти действия должны проходить для владельцев и пользователей системы как можно менее болезненно.



Настроить СЗИ с первого раза не представляется возможным...

Очевидно, что те же действия неоднократно придется повторять администратору безопасности и на этапе эксплуатации системы каждый раз при изменениях состава технических средств, программного обеспечения, персонала и пользователей и т.д. Такие изменения происходят довольно часто, поэтому средства управления системы защиты должны обеспечивать удобство осуществления необходимых при этом изменений настроек системы защиты. Такова “диалектика” применения средств защиты. Если система защиты не учитывает этой диалектики, не обладает достаточной гибкостью и не обеспечивает удобство перенастройки, то такая система очень быстро становится не помощником, а обузой для всех, в том числе и для администраторов безопасности, и обречена на отторжение.

Для поддержки и упрощения действий по настройке средств защиты в системе защиты необходимо предусмотреть следующие возможности:

- выборочное подключение имеющихся защитных механизмов, что обеспечивает возможность реализации режима постепенного поэтапного усиления степени защищенности ИС.
- так называемый “мягкий” режим функционирования средств защиты, при котором несанкционированные действия пользователей (действия с превышением полномочий) фиксируются в системном журнале обычным порядком, но не пресекаются (т.е. не запрещаются системой защиты). Этот режим позволяет выявлять некорректности настроек средств защиты (и затем производить соответствующие их корректировки) без нарушения работоспособности ИС и существующей технологии обработки информации;
- возможности по автоматизированному изменению полномочий пользователя с учетом информации, накопленной в системных журналах (при работе как в “мягком”, так и обычном режимах).

С увеличением масштаба защищаемой ИС усиливаются требования к организации удаленного управления средствами защиты. Поэтому решения, приемлемые для одного автономного компьютера или небольшой сети из 10–15 рабочих станций, совершенно не устраивают обслуживающий персонал (в том числе и администраторов безопасности) больших сетей, объединяющих несколько сотен рабочих станций.

Для решения проблем управления средствами защиты в больших сетях необходимо предусмотреть следующее:

- ***должны поддерживаться возможности управления механизмами защиты*** как централизованно (удаленно, с рабочего места администратора безопасности сети), так и децентрализованно (непосредственно с конкретной рабочей станции). Причем любые измене-

ния настроек защитных механизмов, проведенные централизованно, должны автоматически распространяться на все рабочие станции, которых они касаются (независимо от состояния рабочей станции на момент внесения изменений в центральную базу данных). Аналогично часть изменений, произведенных децентрализованно, должна быть автоматически отражена в центральной базе данных защиты и при необходимости также разослана на все другие станции, которых они касаются. Так, при смене пользователем своего пароля, осуществленной на одной из рабочих станций, новое значение пароля этого пользователя должно быть отражено в центральной базе данных защиты сети, а также разослано на все рабочие станции, где данному пользователю разрешено работать;

- ***управление механизмами защиты конкретной станции*** должно осуществляться независимо от активности данной станции, т.е. независимо от того, включена ли она в данный момент и работает ли на ней пользователь. После включения пассивной станции все изменения настроек, касающиеся ее механизмов защиты, должны быть автоматически перенесены на нее;
- в крупных ИС ***процедура замены версий программ средств защиты*** (как и любых других программ) требует от обслуживающего персонала больших затрат труда и связана с необходимостью обхода всех рабочих станций для получения к ним непосредственного доступа. Проведение таких замен может быть вызвано как необходимостью устранения ошибок в программах, так и потребностью совершенствования и развития системы (установкой новых улучшенных версий программ);
- для больших ИС особую важность приобретает ***оперативный контроль*** за состоянием рабочих станций и работой пользователей в сети. Поэтому система защиты должна включать в себя подсистему оперативного контроля состояния рабочих станций сети и слежения за работой пользователей.

Увеличение количества рабочих станций и использование новых программных средств, содержащих большое количество разнообразных программ (например, MS Windows), приводит к существенному увеличению объема системных журналов регистрации событий, накапливаемых системой защиты. Объем зарегистрированной информации увеличивается настолько, что администратор уже физически не может полностью проанализировать все системные журналы за приемлемое время.

Для облегчения работы администратора должны быть предусмотрены следующие возможности:

- ***подсистема реализации запросов***, позволяющая выбирать из собранных системных журналов данные об определенных событиях (по имени пользователя, дате, времени события, категории происшедшего события и т.п.). Естественно такая подсистема должна опираться на системный механизм обеспечения единого времени событий;
- ***возможность автоматического разбиения и хранения системных журналов*** по месяцам и дням в пределах заданного количества последних дней. Причем во избежание переполнения дисков по истечении установленного количества дней просроченные журналы, если их не удалил администратор, должны автоматически уничтожаться;
- в системе защиты должны быть предусмотрены ***механизмы семантического сжатия данных в журналах регистрации***, позволяющие укрупнять регистрируемые события без существенной потери их информативности. Например, заменять все многократно повторяющиеся в журнале события, связанные с выполнением командного файла autoexec.bat, одним обобщенным. Аналогично можно одним событием заменять многократно повторяющуюся последовательность запуска программ системы MS-Windows и т.п.;
- желательно также иметь в системе ***средства автоматической подготовки отчетных документов*** установленной формы о работе станций сети и имевших место нарушениях. Такие средства позволили бы существенно уменьшить рутинную нагрузку на администрацию безопасности.

Ограничения обработки (650)

Процедуры управления доступом обеспечивают устранение простых угроз от внешних источников, но они не в состоянии препятствовать попыткам проникновения извне, а также попыткам проникновения в систему обслуживающего персонала, нарушающего статус пользователя.

Это важно

Нарушитель, преднамеренно проникнувший в систему, может извлечь, изменить или уничтожить информацию в файлах. Поэтому необходим ввод некоторых ограничений на обработку файлов, содержащих важную информацию. Например, файл, установленный на некотором устройстве, может быть заблокирован для записи информации. Разрешение на выполнение записи дает контроллер файла после установления истинности запроса.

Аналогичные приемы ограничений на обработку могут быть использованы при попытке копировать информацию некоторых файлов или их частей. Одно из эффективных средств борьбы с незаконными обращениями к особо важным файлам — системное уничтожение программы, сформулировавшей запрос. Од-

ним из ограничений при обработке информации является также выделение каждой из выполняемых программ ключей защиты основной памяти.

Функции контроля и управление СЗИ (750)

Эти функции должны обеспечивать:

- ***невозможность разрушения защитного механизма*** системы даже при условии, что пользователь обладает знаниями о технологии его функционирования;
- ***возможность выполнения*** процедур обновления и обработки файлов, а также создания, модификации или исключения данных в тех областях, за которые они отвечают;
- ***время реакции системы*** на запросы пользователя с учетом работы защитного механизма должно быть приемлемым;
- ***система авторизации*** (разрешения доступа) должна налагать допустимые ограничения на работу операционной системы, структуру файлов, техническое обеспечение и систему разделения времени;
- ***возможность выявления*** и использования минимально допустимого списка паролей, ключей и специальных команд с целью упрощения загрузки пользователя при допустимых требованиях к обеспечению и сохранности информации.
- информация, программное обеспечение и коммуникации должны быть ***защищены от неавторизованного доступа*** даже в случае серьезных сбоев аппаратурной части и программного обеспечения;
- ***обеспечение свободного ввода*** данных в файлы, к которым пользователь имеет право доступа;

Контроль за состоянием технической защиты информации (750)

Целью контроля являются выявление возможных технических каналов утечки информативного (опасного) сигнала, выработка мероприятий, обеспечивающих его скрытие, оценка достаточности и эффективности принятых мер защиты, оперативный контроль за состоянием технической защиты каналов утечки информативного сигнала.

Технический канал утечки считается защищенным, если сигнал не превышает установленного нормативной документацией отношения “информативный сигнал/шум”. Устройства защиты и защищенные технические средства считаются исправными, если их параметры соответствуют требованиям эксплуатационных документов.

Контроль за выполнением организационных и подготовительных технических мероприятий по защите информации осуществляется визуальным осмотром прокладки проводов и кабелей, выходящих за пределы объекта защиты, а также технических средств защиты и защищенной техники.

В ходе проверки определяются:

- наличие электромагнитной связи между линиями (прохождение в одном кабеле или жгуте), между разными видами ТС (совместный пробег проводов систем пожарно-охранной сигнализации, часофикации, радиотрансляции);
- наличие выходов линий связи, сигнализации, часофикации, радиотрансляции за пределы выделенных помещений;
- наличие незадействованных ТС, проводов, кабелей;
- возможность отключения ТС на период проведения конфиденциальных переговоров или важных совещаний;
- разнесение источников электромагнитных и акустических полей на максимально возможное расстояние в пределах выделенных помещений;
- выполнение заземления аппаратуры, исключающее возможность образования петель из проводов и экранов;
- разнесение кабелей электропитания ТС с целью исключения наводок опасных сигналов;
- выполнение разводки цепей электропитания экранированным или витым кабелем;
- возможность отключения электропитания ТС при обесточивании сети; отклонение параметров электропитания от норм, заданных в ТУ, при появлении неисправностей в цепях питания.

В процессе проверки эффективности технических мер защиты подвергаются инструментальному контро-

Контроль осуществляется визуальным осмотром...

лю ТС и линии связи. В ходе контроля проверяются электромагнитные поля информативных (опасных) сигналов в широком диапазоне частот вокруг аппаратуры и кабельных соединений ТС, наличие информативных (опасных) сигналов в цепях, проводах электропитания и заземлении ТС.

При проверке определяется радиус, за пределами которого отношение "информативный сигнал/шум" меньше предельно допустимой величины. Проводятся измерение и расчет параметров информативного (опасного) сигнала, выявляется возможность его утечки по каналам ПЭМИН, определяются фактические значения его параметров в каналах утечки, проводится сравнение фактических параметров с нормируемыми.

В случае превышения допустимых значений разрабатываются защитные мероприятия, используются средства защиты (экранирование источников излучения, установка фильтров, стабилизаторов, средств активной защиты).

В процессе работы технических средств и защищенной техники, по мере необходимости, проводится оперативный контроль за эффективностью защиты каналов утечки информативного (опасного) сигнала.

Функции защиты подсистемы управления ИС (050)

Большинство функций защиты подсистемы управления могут быть реализованы как расширенный механизм управления доступом, в котором процессы рассматриваются как ресурсы ИС. К функциям защиты относятся: контроль за порядком следования сообщений, защита программных средств, поддержка взаимодействия недружественных подсистем и реализация процедур с забыванием. ***Для выполнения этих функций модуль защиты должен содержать:***

- информацию о порядке следования;
- некоторое криптографическое преобразование для программной защиты;
- информацию о взаимодействии взаимонедоверяющих подсистем (косвенная идентификация субъектов);
- тесты на проверку условий забывания.

Кроме этих функций модуля контроля и другие функции защиты могут быть реализованы с помощью специальных сетевых протоколов взаимодействия недружественных подсистем или поддержки защиты распределенных вычислений. Все эти механизмы могут быть реализованы путем формирования модуля контроля подсистемы расширенного управления доступом и наполнения соответствующим содержанием структуры, описывающей права доступа.

Интеграция механизмов защиты ИС (650)

Интеграция различных механизмов защиты ИС может быть достигнута при:

- применении одного и того же механизма для различных функций защиты;
- использовании единой концепции построения информационной базы управления защитой;
- использовании унифицированных управляющих функций защиты (управления ключами, проверкой и т.д.);
- формировании единых протоколов взаимодействия пользователей и механизмов защиты и компонентов самого механизма;
- использовании единой стратегии защиты ИС.

Теперь можно сделать вывод о том, что ***информационная база управления защиты должна содержать следующие четыре сегмента (таблицы):***

- параметров защиты пользователя;
- защиты передачи сообщений;
- управления расширенным доступом;
- регистрации.

Все действия должны быть поддержаны специальным сетевым протоколом защиты, который содержит команды с соответствующими параметрами защиты. Интеграция отдельных механизмов защиты достигается путем использования компонентов единой базы управления защитой.

Управление системой защиты следует проводить в несколько этапов:

- провести оценку описанных механизмов защиты;
- выбрать наиболее подходящие для данной сети;
- выявить общие функции управления защитой и формально описать соответствующие механизмы и функции защиты (эта информация послужит основой разработки протоколов защиты ИС);
- выполнить формальную верификацию отдельных механизмов и функций защиты сети.

Все перечисленные этапы составляют теоретическую основу проектирования, реализации, тестирования и применения на практике конкретных сетевых средств защиты, которые должны предоставить пользователям ИС защищенные, надежные и эффективные механизмы реализации сетевых операций.

Управление ключами защиты (754)

Для реализации описанных выше механизмов необходимо добавить некоторые упомянутые ранее функции. Они не связаны непосредственно с защитой сетевых

ресурсов, но содержат некоторые протоколы, данные и структуры, необходимые для эффективного функционирования описанных механизмов. Эти функции содержат то, что называется управлением защитой. Здесь достаточно подробно описан только механизм управления ключами.

Управление ключами защиты в ИС включает следующие функции:

- формирование криптографических ключей;
- распределение, использование, удаление ключей;
- поддержание целостности открытых ключей и защиты личных ключей.

Формирование и распределение криптографических ключей основано на использовании специальных правил и протоколов. Все протоколы используют генераторы случайных чисел и криптографическую защиту ключей, механизмы реализации которых были описаны ранее.

Процедурам удаления, поддержания целостности и защиты криптографических ключей уделяется большое внимание, поскольку защита, целостность и доступность ресурсов ИС в решающей степени зависят от криптографических ключей. Методы защиты секретных ключей, обеспечивающие целостность открытых ключей и защиту ресурсов ИС от компрометации, обязательно должны использовать процедуру текущей регистрации. Для этого ***в базу данных включается таблица регистрации, в разделы которой записываются следующие события:***

- регистрация нового открытого ключа каждого пользователя сети;
- случаи компрометации открытого ключа каждого пользователя;
- образцы сигнатур;
- цифровые сигнатуры и печати.

Каждая запись таблицы регистрации содержит такие элементы:

- тип события,
- идентификатор объекта,
- открытый ключ,
- образец сигнатуры,
- цифровые сигнатуры,
- цифровые печати,
- отметка времени записи.

Если необходима реализация других функций управления защитой, таких, как управление проверкой или восстановление, то это требует введения дополнительных компонентов в информационную базу управления защитой.

Назначение, структура и функции подсистемы управления ключами (754)

Подсистема управления СЗИ предназначена для управления ключами подсистемы криптографической защиты, а также контроля и диагностирования программно-аппаратных средств и обеспечения взаимодействия всех подсистем СЗИ.

Под управлением криптографическими ключами понимаются все действия, связанные с генерацией, распределением, вводом в действие, сменой, хранением, учетом и уничтожением ключей.

К функциям подсистемы относятся:

- управление симметричными ключами шифрования, в которое входит:
- генерация и тестирование ключей симметричного шифрования;
- учет ключей симметричного шифрования и носителей с ними;
- распределение ключей симметричного шифрования;
- контроль за хранением и уничтожением ключей симметричного шифрования;
- контроль за вводом в действие и сменой ключей;
- управление ключами цифровой подписи;
- ведение базы данных открытых ключей (БД ОК) на **центре распределения ключей (ЦРК)**;
- рассылка БД ОК пользователям;

Подсистема управления ключами...

- контроль за вводом в действие и сменой ключей цифровой подписи;
- контроль и диагностирование программно-аппаратных средств защиты.

Структурно подсистема состоит из центра распределения ключей и программно-аппаратных средств, интегрированных в рабочие станции пользователей.

Генерация и тестирование ключей симметричного шифрования (754)

Ключи симметричного шифрования изготавливаются централизованно на ЦРК.

Выработка ключей осуществляется в соответствии с алгоритмами, гарантирующими случайный характер генерируемых ключевых последовательностей. С этой целью на практике наиболее часто применяют аппаратные датчики случайных чисел, в основе которых лежит физический случайный процесс (например, флуктуации напряжения на выходе шумового диода). Кроме того, можно пользоваться датчиками на основе псевдослучайных функций (ДПСЧ), реализующих сгенерированное пользователем секретное начальное значение для инициализации датчика. В таких ДПСЧ возникает проблема генерации случайного начального значения; в качестве источника случайности могут служить временные показатели реакции оператора при диалоге с системой, результат выбора битов из показаний таймера и т.п.

Процесс генерации ключей должен непрерывно и автоматически контролироваться специальными программными средствами с целью обнаружения ошибок и тестирования ключей. Тестирование ключей осуществляется, как правило, по тестам, позволяющим оценить случайность и отбраковать “слабые” ключи. Широкое применение находят статистические тесты (тесты серий, частот, сериальный тест, тест автокорреляции и др.).

Оборудование и процесс генерации ключей должны удовлетворять следующим требованиям:

- компьютеры, оборудованные средствами генерации ключей, должны иметь средства контроля и регистрации доступа;
- генерация ключей должна непрерывно контролироваться соответствующими должностными лицами с целью предотвращения возможности несанкционированного ознакомления с генерируемыми ключами посторонних лиц;
- все документы, сопровождающие процесс генерации ключей, независимо от вида носителя, должны быть надежно защищены от несанкционированного использования, модификации или разрушения;
- пользователи, получающие в распоряжение программно-аппаратные средства генерации ключей, сами несут ответственность за правильность своих действий при генерации, хранении и использовании ключей.

Сгенерированные ключи при необходимости ручной доставки записываются на машинные носители, подлежащие строгому учету. Факт генерации ключей любого типа и записи их на носители отражается в регистрационном журнале ЦРК. Для защиты от возникновения на носителе сбойных участков ключи можно записывать неоднократно. Секретный ключ перед записью на носитель может шифроваться на другом ключе более высокого уровня.

Порядок распределения ключей симметричного шифрования (754)

Распределение ключей в зависимости от их типа осуществляется вручную или в автоматизированном режиме. При ручной доставке ключевые данные предварительно записываются на специальные носители. Ручная доставка должна осуществляться по правилам, принятым для пересылки секретных материалов. При автоматизированной рассылке по каналам связи ключи передаются только в зашифрованном виде.

Порядок распределения симметричных шифрключей определяется ключевой схемой, используемой в системе. При организации засекреченной связи между отдельными парами пользователей (от точки к точке) в простейшем случае для каждой пары вырабатывается свой ключ, доставляемый пользователям вручную; шифрование и дешифрование сообщений выполняется на этом ключе.

В случае двухуровневой схемы шифрование выполняется на сеансовом ключе, который вырабатывает сам пользователь и который действует только в течение одного сеанса связи; при этом сеансовый ключ отправляется вместе с зашифрованным сообщением, но предварительно шифруется на доставленном вручную из ЦРК ключе более высокого уровня.

В трехуровневой схеме главный ключ вырабатывается на ЦРК и рассылается вручную. Затем ЦРК по каналам связи рассылает ключи более низкого уровня (ключи шифрования ключей) в автоматизированном режиме. Пользователь вырабатывает для шифрования сообщений сеансовый ключ и отправляет его вместе с сообщением, предварительно зашифровав на ключе шифрования ключей.

Порядок хранения, доступа и уничтожения ключей симметричного шифрования

Учет носителей с ключевыми данными ведется в журнале регистрации, где отмечается:

- название носителя, отражающее его содержание;
- учетный номер носителя;
- когда на носитель записаны ключевые данные;
- когда и кому носитель выдан;
- подпись лица (пользователя), получившего носитель;
- когда и от кого носитель получен (возвращен);
- дата и подпись (не менее двух должностных лиц ЦРК) об уничтожении ключевых данных на носителе и др.

Учет сформированных на ЦРК ключей ведется в журнальном файле, где отражаются следующие сведения:

- дата формирования ключа;
- его название;
- для кого он сформирован;
- даты ввода в действие и смены (или срок действия);
- сведения об отправке ключа получателю;
- подтверждения получения ключа получателем и др.

Хранение носителей с ключевыми данными организуется в надежных хранилищах (сейфах).

Условия хранения должны исключать:

- возможность незаконного доступа к носителям (кража или порча носителей); ознакомление с их содержанием лиц, не имеющих на это права;
- злонамеренное или случайное изменение их содержания;
- не предусмотренное инструкциями копирование содержимого носителей.

Ключи не следует записывать в открытом виде на носителе, который может быть считан или скопирован.

Уничтожение выведенных из действия ключевых данных на магнитных носителях осуществляется с помощью программ уничтожения остаточной информации. Уничтожение выведенных из действия ключевых данных на других носителях производится по соответствующим руководствам. Неисправные носители с ключевыми данными уничтожаются физически. Уничтожение выполняет оператор ЦРК в присутствии администратора ЦРК. Факт уничтожения фиксируется в регистрационном журнале и заверяется их подписями.

Доступ к ключам имеют только должностные лица ЦРК и ограниченный круг пользователей, ответственных за хранение и использование носителей с ключами. ***Кроме того, доступ к ключам ограничивается техническими мерами:***

- сеансовый ключ в процессе его формирования и использования должен быть скрыт от пользователя;
- ключи не хранятся, как правило, в открытом виде;
- ключ записывается только на съемные носители, устанавливаемые в ЭВМ на период его использования.

Управление ключами несимметричного криптопреобразования (754)

Секретный ключ ключевой пары после его выработки хранится у владельца и никому не пересылается.

Открытый ключ должен быть известен всем санкционированным пользователям для возможности проверки цифровой подписи. Распределение открытых ключей проводится различными методами: с использованием центра распределения ключей (ЦРК) или путем пересылки вместе с подписанным сообщением.

В первом случае выработанный пользователем открытый ключ цифровой подписи регистрируется им в ЦРК, которым является доверенный источник сети, для формирования сводной базы данных открытых ключей (БД ОК). Все санкционированные пользователи имеют доступ к БД ОК или получают ее при первоначальной регистрации в системе. При смене ключей цифровой подписи каким-либо пользователем новый открытый ключ рассылается остальным пользователям по установленному каналу связи. Во втором случае открытый ключ добавляется к подписанному сообщению.

Варианты реализации управления ключами в СЗИ (754)

В СЗИ управление ключами целесообразно возложить на центр распределения ключей. ***ЦРК осуществляет:***

- централизованную генерацию симметричных шифрключей, их распределение и контроль за дальнейшим использованием;
- ведение и рассылку базы данных открытых ключей;
- контроль за использованием несимметричных ключей;
- ведение архивов открытых ключей цифровой подписи;
- участие в предварительной проверке спорных ситуаций, возникающих при использовании цифровой подписи;
- разработку мероприятий на случай компрометации ключей;
- гарантированное стирание ключевых данных на носителях по истечении срока действия ключей.

В качестве ключевой схемы целесообразно выбрать двухуровневую (главный ключ, формируемый на ЦРК, и сеансовый ключ, формируемый пользователем).

Ключи цифровой подписи рекомендуется формировать самим пользователям, чтобы не создавать проблему доверия к ЦРК. ЦРК осуществляет управление открытыми ключами цифровой подписи. При этом формируется база данных открытых ключей, которая рассылается всем пользователям ИС, использующим цифровые подписи. ЦРК следит за обновлением базы, контролирует ввод в действие и срок действия ключей цифровой подписи, разрабатывает мероприятия на случай компрометации ключей.

Резюме

Управление защитой — это контроль за распределением информации в информационных системах. Он осуществляется для обеспечения функционирования средств и механизмов защиты; фиксации выполняемых функций и состояний механизмов защиты, а также событий, связанных с нарушением защиты.

Настройка средств защиты, управление системой защиты и осуществление контроля функционирования ИС — все это составляющие одной задачи — реализации политики безопасности.

Управление средствами защиты включает в себя несколько задач и их правильное решение способствует успешному функционированию ИС в целом. При этом, как правило, ни одна из крайностей — тотальная защита или полное ее отсутствие — не способствует оптимальной работе.

Настройка средств защиты необходима для приведения средств защиты информации в соответствие с разработанным планом. При настройке добавленных средств защиты необходимо особое внимание уделить вопросам проверки их совместимости с используемыми прикладными программами.

Управление системой защиты состоит в периодическом внесении изменений в базу данных защиты, содержащую сведения о пользователях, допущенных к работе в системе, их правах доступа к различным объектам системы и др.

Особое внимание при управлении системой защиты необходимо обратить на следующее:

- документированность всех изменений в базе данных защиты. Лучше всего организовать систему заявок от должностных лиц организации на разрешение доступа тому или иному сотруднику организации к какому-либо ресурсу системы. При этом ответственность за допуск сотрудника возлагается на соответствующее лицо, подписавшее заявку;
- периодическое резервное копирование базы данных защиты во избежание утраты их актуальной копии в случае сбоя (отказа) оборудования;

Контроль за функционированием ИС заключается в слежении за опасными событиями, анализе причин, которые привели к их возникновению и устранению последствий (если таковые наступили).

Как правило, задачи управления и контроля решаются административной группой, количественный и личный состав которой зависят от конкретных условий. Обычно в эту группу входят: администратор безопасности, менеджер безопасности и операторы.

Организация группы управления защитой информации, включающей специалистов в этой области — одна из наиболее важных задач управления защитой ИС. Иногда эту группу называют группой информационной безопасности.

Процедуры управления доступом обеспечивают устранение простых угроз от внешних источников, но они не в состоянии препятствовать попыткам проникновения извне, а также попыткам проникновения в систему обслуживающему персоналу, нарушающему статус пользователя.

Нарушитель, преднамеренно проникнувший в систему, может извлечь, изменить или уничтожить информацию в файлах. Поэтому необходим ввод некоторых ограничений на обработку файлов, содержащих важную информацию.

Чтобы получить информацию о каком-либо объекте ИС, вовсе не обязательно искать пути несанкционированного доступа к нему. Можно получать информацию, наблюдая за работой системы и, в частности, за обработкой требуемого объекта. Иными словами, при помощи каналов утечки информации.