ОГЛАВЛЕНИЕ

1 ФОРМИРОВАНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ. ....... 3 2 Полномочная политика безопасности .................................................................... 6 3 Управление доступом .............................................................................................. 7 4 Политика ИБ Газпромбанка .................................................................................. 12 5 Политика информационной и экономической безопасности оао «радиотехнический институт имени академика А.Л. Минца» .................................. 25 6 Задание по составлению политики ИБ ................................................................. 26

1 ФОРМИРОВАНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ.

Политика безопасности представляет собой некоторый набор требований, прошедших соответствующую проверку, реализуемых при помощи организационных мер и программно-технических средств и определяющих архитектуру системы защиты. Ее реализация для конкретной автоматизированной системы обработки информации осуществляется при помощи средств управления механизмами защиты. Для конкретной организации политика безопасности должна быть индивидуальной, зависимой от конкретной технологии обработки информации, используемых программных и технических средств, расположения организации и т.д. Политика безопасности — документ «верхнего» уровня, в котором должны быть указаны: • лица, ответственные за безопасность функционирования организации; • полномочия и ответственность отделов и служб в отношении безопасности; • организация допуска новых сотрудников и их увольнения; • правила разграничения доступа сотрудников к информационным ресурсам; • организация пропускного режима, регистрации сотрудников и посетителей; • использование программно-технических средств защиты; • другие требования общего характера. Политика безопасности — это организационно-правовой и технический документ одновременно. Любая защитная мера есть компромисс между снижением рисков и удобством работы пользователя.

Т.е. политика безопасности нужна для определения основных понятий и

направления деятельности в обеспечении ИБ в организации. Она становится тем документом, на основании которого составляются регламенты и инструкции. ПИБ составляется для всех сотрудников организации, поэтому конечные пользователи и топ-менеджмент компании должны понять смысл написанного в ПИБ. Под "системой" понимается некоторая совокупность субъектов и объектов и отношения между ними:  Субъект - активный компонент системы, который может явиться причиной потока информации от объекта к субъекту или изменения состояния системы.  Объект - пассивный компонент системы, хранящий, принимающий или передающий информацию. Доступ к объекту подразумевает доступ к содержащейся в нем информации. Основу политики безопасности составляет способ управления доступом, определяющий порядок доступа субъектов системы к объектам системы. Название данного способа, как правило, определяет название политики безопасности. В настоящее время лучше всего изучены два вида политики безопасности: избирательная и полномочная, основанные, соответственно на избирательном и полномочном способах управления доступом. Определение прав доступа субъектов к объектам и/или информационным потокам (полномочий субъектов и атрибутов объектов, присвоение меток критичности и т.д.) входит в компетенцию администрации системы. Избирательная политика Основой избирательной политики безопасности является избирательное управление доступом (ИУД, Discretionary Access Control; DAC), которое подразумевает, что:  все субъекты и объекты системы должны быть идентифицированы;  права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности). Для описания свойств избирательного управления доступом применяется модель

системы на основе матрицы доступа (МД, иногда ее называют матрицей контроля доступа). Такая модель получила название матричной. Матрица доступа представляет собой матрицу, в которой объекту системы соответствует столбец, а субъекту - строка. На пересечении столбца и строки матрицы указывается тип (типы) разрешенного доступа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту как "доступ на чтение", "доступ на запись", "доступ на исполнение" и др. Множество объектов и типа доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе. Определение и изменение этих правил также является задачей ИУД. Например, доступ субъекта к конкретному объекту может быть разрешен только в определенные дни (дата - зависимое условие), часы (время - зависимое условие), в зависимости от других характеристик субъекта (контекстно-зависимое условие) или в зависимости от характера предыдущей работы. Такие условия на доступ к объектам обычно используются в СУБД. Кроме того, субъект с определенными полномочиями может передавать их другому субъекту (если это не противоречит правилам политики безопасности). Решение на доступ субъекта к объекту принимается в соответствии с типом доступа, указанным в соответствующей ячейке матрицы доступа. Обычно, избирательное управление доступом реализует принцип "что не разрешено, то запрещено", предполагающий явное разрешение доступа субъекта к объекту. Матрица доступа - наиболее примитивный подход к моделированию систем, который, однако, является основой для более сложных моделей, наиболее полно описывающих различные стороны реальных автоматизированных систем обработки информации. Вследствие больших размеров и разреженности МД хранение полной матрицы представляется нецелесообразным, поэтому во многих средствах защиты используют более экономные представления МД (профили и т. д.). Каждый из этих способов представления МД имеет свои достоинства и свои недостатки, обуславливающие область их применения. Поэтому в каждом конкретном случае

надо знать, во-первых, какое именно представление использует средство защиты, и, во-вторых, какие особенности и свойства имеет это представление. Избирательная политика безопасности наиболее широко применяется в коммерческом секторе, так как ее реализация на практике отвечает требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость и небольшие накладные расходы.

2 ПОЛНОМОЧНАЯ ПОЛИТИКА БЕЗОПАСНОСТИ

Основу полномочной политики безопасности составляет полномочное управление доступом (Mandatory Access Control; MAC), которое подразумевает, что:  все субъекты и объекты системы должны быть однозначно идентифицированы;  каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;  каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ. В том случае, когда совокупность меток имеет одинаковые значения, говорят, что они принадлежат к одному уровню безопасности. Организация меток имеет иерархическую структуру и, таким образом, в системе можно реализовать иерархически не нисходящий (по ценности) поток информации (например, от рядовых исполнителей к руководству). Чем важнее объект или субъект, тем выше его метка критичности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки критичности. Каждый субъект кроме уровня прозрачности имеет текущее значение уровня безопасности, которое может изменяться от некоторого минимального значения до значения его уровня прозрачности. Для моделирования полномочного управления доступом используется модель

Белла-Лападула (Bell-LaPadulla model), включающая в себя понятие безопасного (с точки зрения политики) состояния и перехода. Для принятия решения на разрешение доступа производится сравнение метки критичности объекта с уровнем прозрачности и текущим уровнем безопасности субъекта. Результат сравнения определяется двумя правилами: простым условием защиты (simple security condition) и \*-свойством (\*-property). В упрощенном виде, они определяют, что информация может передаваться только "наверх", то есть субъект может читать содержимое объекта, если его текущий уровень безопасности не ниже метки критичности объекта, и записывать в него, - если не выше (\*-свойство). Простое условие защиты гласит, что любую операцию над объектом субъект может выполнять только в том случае, если его уровень прозрачности не ниже метки критичности объекта. Основное назначение полномочной политики безопасности - регулирование доступа субъектов системы к объектам с различным уровнем критичности и предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние. При этом она функционирует на фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности).

3 УПРАВЛЕНИЕ ДОСТУПОМ

Основные понятия С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами). В данном разделе речь идет о логическом управлении доступом, которое, в отличие от физического, реализуется программными средствами. Логическое управление доступом - это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

Рассмотрим формальную постановку задачи в традиционной трактовке. Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары "субъект-объект" определить множество допустимых операций (зависящее, быть может, от некоторых дополнительных условий) и контролировать выполнение установленного порядка. Отношение "субъекты-объекты" можно представить в виде матрицы доступа, в строках которой перечислены субъекты, в столбцах - объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа. Фрагмент матрицы может выглядеть, например, так:

Таблица 10.1. Фрагмент матрицы доступа

Файл Программа Линия связи Реляционная таблица

Пользователь 1 orw с системной консоли

e rw с 8:00 до 18:00

Пользователь 2

a

"o" - обозначает разрешение на передачу прав доступа другим пользователям, "r" - чтение, "w" - запись, "e" - выполнение, "a" - добавление информации Тема логического управления доступом - одна из сложнейших в области информационной безопасности. Дело в том, что само понятие объекта (а тем более видов доступа) меняется от сервиса к сервису. Для операционной системы к объектам относятся файлы, устройства и процессы. Применительно к файлам и устройствам обычно рассматриваются права на чтение, запись, выполнение (для программных файлов), иногда на удаление и добавление. Отдельным правом может быть возможность передачи полномочий доступа другим субъектам (так называемое право владения). Процессы можно создавать и уничтожать. Современные

операционные системы могут поддерживать и другие объекты. Для систем управления реляционными базами данных объект - это база данных, таблица, представление, хранимая процедура. К таблицам применимы операции поиска, добавления, модификации и удаления данных, у других объектов иные виды доступа. Разнообразие объектов и применимых к ним операций приводит к принципиальной децентрализации логического управления доступом. Каждый сервис должен сам решать, позволить ли конкретному субъекту ту или иную операцию. Теоретически это согласуется с современным объектноориентированным подходом, на практике же приводит к значительным трудностям. Главная проблема в том, что ко многим объектам можно получить доступ с помощью разных сервисов (возможно, при этом придется преодолеть некоторые технические трудности). Так, до реляционных таблиц можно добраться не только средствами СУБД, но и путем непосредственного чтения файлов или дисковых разделов, поддерживаемых операционной системой (разобравшись предварительно в структуре хранения объектов базы данных). В результате при задании матрицы доступа нужно принимать во внимание не только принцип распределения привилегий для каждого сервиса, но и существующие связи между сервисами (приходится заботиться о согласованности разных частей матрицы). Аналогичная трудность возникает при экспорте/импорте данных, когда информация о правах доступа, как правило, теряется (поскольку на новом сервисе она не имеет смысла). Следовательно, обмен данными между различными сервисами представляет особую опасность с точки зрения управления доступом, а при проектировании и реализации разнородной конфигурации необходимо позаботиться о согласованном распределении прав доступа субъектов к объектам и о минимизации числа способов экспорта/импорта данных. При принятии решения о предоставлении доступа обычно анализируется следующая информация:

 идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера и т.п.). Подобные идентификаторы являются основой произвольного (или дискреционного) управления доступом;  атрибуты субъекта (метка безопасности, группа пользователя и т.п.). Метки безопасности - основа принудительного (мандатного) управления доступом. Матрицу доступа, ввиду ее разреженности (большинство клеток - пустые), неразумно хранить в виде двухмерного массива. Обычно ее хранят по столбцам, то есть для каждого объекта поддерживается список "допущенных" субъектов вместе с их правами. Элементами списков могут быть имена групп и шаблоны субъектов, что служит большим подспорьем администратору. Некоторые проблемы возникают только при удалении субъекта, когда приходится удалять его имя из всех списков доступа; впрочем, эта операция производится нечасто. Списки доступа - исключительно гибкое средство. С их помощью легко выполнить требование о гранулярности прав с точностью до пользователя. Посредством списков несложно добавить права или явным образом запретить доступ (например, чтобы наказать нескольких членов группы пользователей). Безусловно, списки являются лучшим средством произвольного управления доступом. Подавляющее большинство операционных систем и систем управления базами данных реализуют именно произвольное управление доступом. Основное достоинство произвольного управления - гибкость. Вообще говоря, для каждой пары "субъект-объект" можно независимо задавать права доступа (особенно легко это делать, если используются списки управления доступом). К сожалению, у "произвольного" подхода есть ряд недостатков. Рассредоточенность управления доступом ведет к тому, что доверенными должны быть многие пользователи, а не только системные операторы или администраторы. Из-за рассеянности или некомпетентности сотрудника, владеющего секретной информацией, эту информацию могут узнать и все остальные пользователи. Следовательно, произвольность управления должна быть дополнена жестким контролем за реализацией избранной политики безопасности.

Второй недостаток, который представляется основным, состоит в том, что права доступа существуют отдельно от данных. Ничто не мешает пользователю, имеющему доступ к секретной информации, записать ее в доступный всем файл или заменить полезную утилиту ее "троянским" аналогом. Подобная "разделенность" прав и данных существенно осложняет проведение несколькими системами согласованной политики безопасности и, главное, делает практически невозможным эффективный контроль согласованности.

4 ПОЛИТИКА ИБ ГАЗПРОМБАНКА

Общие положения включают перечисление нормативных документов, на основании которых создана политика безопасности, назначение документа, взгляды руководства Банка на обеспечение ИБ, на риски ИБ, нормативную базу для выполнения стратегии ЗИ, целевую аудиторию, взаимодействие с другими организациями и дочерними компаниями.

Список терминов и определений описывает понятийный аппарат.

Описание объекта защиты содержит указание субъектов и объектов ЗИ.

Угрозы информационной безопасности классифицированы на 3 класса и описаны, построена модель нарушителя ИБ (внутреннего и внешнего).

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия. Источники угроз по отношению к инфраструктуре Банка могут быть как внешними, так и внутренними.

Основные положения по обеспечению ИБ в Банке включают порядок управления рисками ИБ, инцидентами ИБ, защиту от утечек по техническим каналам, проверки по ИБ.

В разделе Организационная основа описаны роли по информационной безопасности в Банке.

Кроме того, Политика определяет ответственность и контроль за соблюдением соответствующих положений.

5 ПОЛИТИКА ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ОАО «РАДИОТЕХНИЧЕСКИЙ ИНСТИТУТ ИМЕНИ АКАДЕМИКА А.Л. МИНЦА»

Как видно из содержания документа структура ПБ и содержание несколько отличается, но есть общие моменты, присущие обеим ПБ. В частности, описание объектов защиты, термины и определения, угрозы безопасности, цели и задачи ИБ, порядок реализации ПБ, ответственные лица и порядок осуществления контроля за соблюдением ПБ.

6 ЗАДАНИЕ ПО СОСТАВЛЕНИЮ ПОЛИТИКИ ИБ

Например, Компания ООО «Солнышко». Штат — 50 сотрудников. 5 руководство, 5 бухгалтерия, 5 — IT-отдел, 30 — менеджеры по работе с клиентами, 5 — отдел безопасности. Управление компании использует телефонную связь, MS Office, 1С: Предприятие и т. д.

Бухгалтерия использует телефонную связь, MS Office, 1С: Бухгалтерию. IT-отдел обеспечивает функционирование внутренней сети организации, а также сайта компании и личных кабинетов клиентов. Менеджеры по работе с клиентами осуществляют работу с ними посредством Интернет. Телефонной связи и др. Задача: составить политику информационной безопасности для организации. Составить технический регламент, инструкцию для одного из отделов.