**Информационная безопасность банков**

Информационная безопасность банка должна учитывать следующие специфические факторы:

1. Хранимая и обрабатываемая в банковских системах информация представляет собой реальные деньги. На основании информации компьютера могут производится выплаты, открываться кредиты, переводиться значительные суммы. Вполне понятно, что незаконное манипулирование с такой информацией может привести к серьезным убыткам. Эта особенность резко расширяет круг преступников, покушающихся именно на банки (в отличие от, например, промышленных компаний, внутренняя информация которых мало кому интересна).

2. Информация в банковских системах затрагивает интересы большого количества людей и организаций — клиентов банка. Как правило, она конфиденциальна, и банк несет ответственность за обеспечение требуемой степени секретности перед своими клиентами. Естественно, клиенты вправе ожидать, что банк должен заботиться об их интересах, в противном случае он рискует своей репутацией со всеми вытекающими отсюда последствиями.

3. Конкурентоспособность банка зависит от того, насколько клиенту удобно работать с банком, а также насколько широк спектр предоставляемых услуг, включая услуги, связанные с удаленным доступом. Поэтому клиент должен иметь возможность быстро и без утомительных процедур распоряжаться своими деньгами. Но такая легкость доступа к деньгам повышает вероятность преступного проникновения в банковские системы.

4. Информационная безопасность банка (в отличие от большинства компаний) должна обеспечивать высокую надежность работы компьютерных систем даже в случае нештатных ситуаций, поскольку банк несет ответственность не только за свои средства, но и за деньги клиентов.

5. Банк хранит важную информацию о своих клиентах, что расширяет круг потенциальных злоумышленников, заинтересованных в краже или порче такой информации.

Преступления в банковской сфере также имеют свои особенности [2, с.16]:

* Многие преступления, совершенные в финансовой сфере остаются неизвестными для широкой публики в связи с тем, что руководители банков не хотят тревожить своих акционеров, боятся подвергнуть свою организацию новым атакам, опасаются подпортить свою репутацию надежного хранилища средств и, как следствие, потерять клиентов.

Преступления в банковской сфере также имеют свои особенности [2. с. 16]:  
• Многие преступления, совершенные в финансовой сфере остаются  
неизвестными для широкой публики в связи с тем. что руководители банков  
не хотят тревожить своих акционеров, боятся подвергнуть свою  
организацию новым атакам, опасаются подпортить свою репутацию  
надежного хранилища средств и. как следствие, потерять клиентов.

• Как правило, злоумышленники обычно используют свои собственные счета,  
на который переводятся похищенные суммы. Большинство преступников не  
знают, как «отмыть» украденные деньги. Умение совершить преступление и  
умение получить деньги — это не одно и то же.

• Большинство компьютерных преступлений — мелкие. Ущерб от них -лежит  
в интервале от S10.000 до S50.000.

• Успешные компьютерные преступления, как правило, требуют большого  
количества банковских операций (до нескольких сотен). Однако крупные  
суммы могут пересылаться и всего за несколько транзакций.

• Большинство злоумышленников — клерки. Хотя высший персонал банка  
также может совершать преступления и нанести банку гораздо больший  
ущерб — такого рода случаи единичны.

• Компьютерные преступления не всегда высокотехнологичны. Достаточно  
подделки данных, изменения параметров среды АСОИБ и т.д.. а эти  
действия доступны и обслуживающему персоналу.

• Многие злоумышленники объясняют свои действия тем. что они всего лишь  
берут в долг у банка с последующим возвратом. Впрочем «возврата», как  
правило, не происходит.

**Специфика защиты автоматизированных систем обработки информации банков (АСОИБ)** обусловлена особенностями решаемых ими задач:

• Как правило АСОИБ обрабатывают большой поток постоянно поступающих  
запросов в реальном масштабе времени, каждый из которых не требует для  
обработки многочисленных ресурсов, но все вместе они могут быть  
обработаны только высокопроизводительной системой;

• В АСОИБ хранится и обрабатывается конфиденциальная информация, не  
предназначенная для широкой публики. Ее подделка или утечка могут  
привести к серьезным (для банка или его клиентов) последствиям. Поэтому  
АСОИБ обречены оставаться относительно закрытыми, работать под  
управлением специфического программного обеспечения и уделять большое  
внимание обеспечению своей безопасности; \_

• Другой особенностью АСОИБ является повышенные требования к  
надежности аппаратного и программного обеспечения. В силу этого многие  
современные АСОИБ тяготеют к так называемой отказоустойчивой  
архитектуре компьютеров, позволяющей осуществлять непрерывную  
обработку информации даже в условиях различных сбоев и отказов.

**Можно выделить два типа задач, решаемых АСОИБ:|**

1. Аналитические. К этому типу относятся задачи планирования, анализа счетов и т.д. Они не являются оперативными и могут требовать для решения длительного времени, а их результаты могут оказать влияние на политику банка в отношении конкретного клиента или проекта. Поэтому подсистема, с помощью которой решаются аналитические задачи, должна быть надежно изолирована от основной системы обработки информации. Для решения такого рода задач обычно не требуется мощных вычислительных ресурсов, обычно достаточно 10-20% мощности всей системы. Однако ввиду возможной ценности результатов их защита должна быть постоянной.

2. Повседневные. К этому типу относятся задачи, решаемые в повседневной деятельности, в первую очередь выполнение платежей и корректировка счетов. Именно они и определяют размер и мощность основной системы банка; для их решения обычно требуется гораздо больше ресурсов, чем для аналитических задач. В то же время ценность информации, обрабатываемой при решении таких задач, имеет временный характер. Постепенно ценность информации, например, о выполнении какого-либо платежа, становиться не актуальной. Естественно, это зависит от многих факторов, как-то: суммы и времени платежа, номера счета, дополнительных характеристик и т.д. Поэтому, обычно бывает достаточным обеспечить защиту платежа именно в момент его осуществления. При этом защита самого процесса обработки и конечных результатов должна быть постоянной.

Каким же мерам защиты систем обработки информации отдают предпочтение зарубежные специалисты? На этот вопрос можно ответить, используя результаты опроса, проведенного Datapro Information Group в 1994 году среди банков и финансовых организаций [2]:

* Сформулированную политику информационной безопасности имеют 82% опрошенных. По сравнению с 1991 годом процент организаций, имеющих политику безопасности, увеличился на 13%.
* Еще 12% опрошенных планируют разработать политику безопасности. Четко выражена следующая тенденция: организации с большим числом персонала предпочитают иметь разработанную политику безопасности в большей степени, чем организации с небольшим количеством персонала. Например, по данным этого опроса, всего лишь 66% организаций, с числом сотрудников менее 100 человек имеют политику безопасности, тогда как для организаций с числом сотрудников более 5000 человек доля таких организаций составляет 99%.
* В 88% организаций, имеющих политику информационной безопасности, существует специальное подразделение, которое отвечает за ее реализацию. В тех организациях, которые не содержат такое подразделение, эти функции, в основном, возложены на администратора системы (29%), на менеджера информационной системы (27%) или на службу физической безопасности (25%). Это означает, что существует тенденция выделения сотрудников, отвечающих за компьютерную безопасность, в специальное подразделение.
* В плане защиты особое внимание уделяется защите компьютерных сетей (90%), больших ЭВМ (82%), восстановлению информации после аварий и катастроф (73%), защите от компьютерных вирусов (72%), защите персональных ЭВМ (69%).

Можно сделать следующие выводы об особенностях защиты информации в зарубежных финансовых системах [2, с.21]:

• Главное в защите финансовых организаций — оперативное и по  
возможности полное восстановление информации после аварий и сбоев.  
Около 60% опрошенных финансовых организаций имеют план такого  
восстановления, который ежегодно пересматривается в более чем 80% из  
них. В основном, защита информации от разрушения достигается созданием  
резервных копий и их внешним хранением, использованием средств  
бесперебойного электропитания и организацией «горячего» резерва  
аппаратных средств.

• Следующая по важности для финансовых организаций проблема — это  
управление доступом пользователей к хранимой и обрабатываемой  
информации. Здесь широко используются различные программные системы  
управления доступом, которые иногда могут заменять и антивирусные  
программные средства. В основном используются приобретенные  
программные средства управления доступом. Причем в финансовых  
организациях особое внимание уделяют такому управлению пользователей  
именно в сети. Однако сертифицированные средства управления доступом  
встречаются крайне редко (3%). Это можно объяснить тем. что с  
сертифицированными программными средствами трудно работать и они  
крайне дороги в эксплуатации. Это объясняется тем. что параметры  
сертификации разрабатывались с учетом требований, предъявляемым к  
военным системам.

• К отличиям организации защиты сетей ЭВМ в финансовых организациях  
можно отнести широкое использование стандартного (т.е. адаптированного,  
но не специально разработанного для конкретной организации)  
коммерческого программного обеспечения для управления доступом к сети  
(82%). защита точек подключения к системе через коммутируемые -линии  
связи (69%). Скорее всего это связано с большей распространенностью  
средств телекоммуникаций в финансовых сферах и желание защититься от  
вмешательства извне. Другие способы защиты, такие как применение  
антивирусных средств, оконечное и канальное шифрование передаваемых  
данных, аутентификация сообщений применяются примерно одинаково и. в  
основном (за исключением антивирусных средств), менее чем в 50%  
опрошенных организаций.

• Большое внимание в финансовых организациях уделяется физической  
защите помещений, в которых расположены компьютеры (около 40%). Это  
означает, что защита ЭВМ от доступа посторонних лиц решается не только с  
помощью программных средств, но и организационно-технических (охрана,  
кодовые замки и т.д.).

• Шифрование локальной информации применяют чуть более 20%  
финансовых организаций. Причинами этого являются сложность  
распространения ключей, жесткие требования к быстро действию системы, а  
также необходимость оперативного восстановления информации при сбоях  
и отказах оборудования.

• Значительно меньшее внимание в финансовых организациях уделяется  
защите телефонных линий связи (4%) и использованию ЭВМ.  
разработанных с учетом требования стандарта Tempest (защита от утечки  
информации по каналам электромагнитных излучений и наводок). В  
государственных организациях решению проблемы противодействия  
получению информации с использованием электромагнитных излучений и  
наводок уделяют гораздо большее внимание.

**Анализ статистики позволяет сделать важный вывод: защита финансовых организаций (в том числе и банков) строится несколько иначе, чем обычных коммерческих и государственных организаций. Следовательно для защиты АСОИБ нельзя применять те же самые технические и организационные решения, которые были разработаны для стандартных ситуаций. Нельзя бездумно копировать чужие системы — они разрабатывались для иных условий.**

**Человеческий фактор в обеспечении информационной безопасности.**

Можно выделять четыре основные причины нарушений по вине человеческого фактора: безответственность, самоутверждение, месть и корыстный интерес пользователей (персонала) АСОИБ.

При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности. Маловероятно, чтобы разработчики системы защиты могли предусмотреть все такие ситуации. Более того, во многих случаях система в принципе не может предотвратить подобные нарушения (например, случайное уничтожение своего собственного набора данных). Иногда ошибки поддержки адекватной защищенной среды могут поощрять такого рода нарушения. Даже лучшая система защиты будет скомпрометирована, если она неграмотно настроена. Наряду с неподготовленностью пользователей к точному соблюдению мер защиты, это обстоятельство может сделать систему уязвимой к этому виду нарушений.

Некоторые пользователи считают получение доступа к системным наборам данных крупным успехом, затевая своего рода игру «пользователь против системы» ради самоутверждения либо всобственных глазах, либо в глазах коллег. Хотя намерения могут быть и безвредными, эксплуатация ресурсов АСОИБ считается нарушением политики безопасности. Пользователи с более серьезными намерениями могут найти конфиденциальные данные, попытаться испортить или уничтожить их при этом. Такой вид нарушения называется **зондированием** системы. Большинство систем имеет ряд средств противодействия подобным «шалостям». В случае необходимости администратор защиты использует их временно или постоянно.

Нарушение безопасности АСОИБ может быть вызвано и **корыстным интересом** пользователя системы. В этом случае он будет целенаправленно пытаться преодолеть систему защиты для доступа к хранимой, передаваемой иобрабатываемой в АСОИБ информации. Даже если АСОИБ имеет средства, делающие такое проникновение чрезвычайно сложным, полностью защитить ее от проникновения практически невозможно. Тот, кому успешно удалось **проникновение** — очень квалифицирован и опасен. Проникновение — опаснейший вид нарушений, правда, он встречается чрезвычайно редко, так как требуют необычайного мастерства и упорства.

Как показывает практика, ущерб от каждого вида нарушений обратно пропорционален его частоте: чаще всего встречаются нарушения, вызванные халатностью и безответственностью, обычно ущерб от них незначителен и легко восполняется. Например, случайно уничтоженный набор данных можно восстановить, если сразу заметить ошибку. Если информация имеет важное значение, то необходимо хранить регулярно обновляемую резервную копию, тогда ущерб вообще практически незаметен.

Ущерб от зондирования системы может быть гораздо больше, но и вероятность его во много раз ниже. Для таких действий необходима достаточно высокая квалификация, отличное знание системы защиты и определенные психологические особенности. Наиболее характерным результатом зондирования системы является блокировка: пользователь в конце концов вводит АСОИБ в состояние зависания, после чего операторы и системные программисты должны тратить много времени для восстановления работоспособности системы.

**Проникновение** — наиболее редкий вид нарушений, но и наиболее опасный. Отличительной чертой проникновении обычно является определенная цель: доступ (чтение, модификация, уничтожение) к определенной информации, влияние на работоспособность системы, слежение за действиями других пользователей и др. Для выполнения подобных действий нарушитель должен обладать теми же качествами, что и для зондирования системы, только в усиленном варианте, а также иметь точно сформулированную цель. В силу этих обстоятельств ущерб от проникновении может оказаться в принципе невосполнимым. Например, для банков это может быть полная или частичная модификация счетов с уничтожением журнала транзакций.

Таким образом, для организации надежной защиты необходимо четко отдавать себе отчет, от каких именно нарушений важнее всего избавиться, Для защиты от нарушений, вызванных халатностью нужна минимальная защита, для защиты от зондирования системы — более жесткая и самая жесткая вместе с постоянным контролем — от проникновении. Целью таких действий должно служить одно — обеспечение работоспособности АСОИБ в целом и ее системы защиты в частности.

Причины, побудившие пользователя совершить нарушение или даже преступление, могут быть совершенно различными. Как уже отмечалось, около 86% нарушений составляют неумышленные ошибки, вызванные небрежностью, недостаточной компетентностью, безответственностью и т.д. Но не это составляет основную угрозу для системы. Гораздо более серьезным может быть ущерб, нанесенный в результате умышленного воздействия из-за обиды, неудовлетворенности своим служебным или материальным положением или по указанию других лиц. Причем ущерб этот будет тем больше, чем выше положение пользователя в служебной иерархии. Это только некоторые из возможных причин, побуждающих пользователей идти на нарушение правил работы с системой.

Способы предотвращения нарушений вытекают из природы побудительных мотивов — это соответствующая подготовка пользователей, а также поддержание здорового рабочего климата в коллективе, подбор персонала, своевременное обнаружение потенциальных злоумышленников и принятие соответствующих мер. Первая из них - задача администрации системы, вторая — психолога и всего коллектива в целом. Только в случае сочетания этих мер имеется возможность не исправлять нарушения и не расследовать преступления, а предотвращать саму их причину.

При создании модели нарушителя и оценке риска потерь от действий персонала необходимо дифференцировать всех сотрудников по их возможностям доступа к системе и, следовательно, по потенциальному ущербу от каждой категории пользователей. Например, оператор или программист автоматизированной банковской системы может нанести несравненно больший ущерб, чем обычный пользователь, тем более непрофессионал.

Ниже приводится примерный список персонала типичной АСОИБ и соответствующая **степень риска** от каждого из них [3].

1. Наибольший риск:

- системный контролер;

- администратор безопасности.

2. Повышенный риск:

- оператор системы;

- оператор ввода и подготовки данных;

- менеджер обработки;

- системный программист.

3. Средний риск:

- инженер системы;

- менеджер программного обеспечения.

4. Ограниченный риск:

- прикладной программист;

- инженер или оператор по связи;

- администратор баз данных;

- инженер по оборудованию;

- оператор периферийного оборудования;

- библиотекарь системных магнитных носителей;

- пользователь-программист;

- пользователь-операционист.

5. Низкий риск:

- инженер по периферийному оборудованию;

- библиотекарь магнитных носителей пользователей;

- пользователь сети.

Каждый из перечисленных выше пользователей в соответствии со своей категорией риска может нанести больший или меньший ущерб системе. Однако пользователи различных категорий различаются не только по степени риска, но и по тому, какому элементу системы они угрожают больше всего. Понятно, что операционист вряд ли сможет вывести из строя АСОИБ, но зато способен послать платеж не по адресу и нанести серьезный финансовый ущерб.

**В настоящее время** ведущие банковские струк­туры имеют, как правило, строго разработанные и ут­вержденные руководством организационные структу­ры и функции управления для каждого подразделения. Наибольшей популярностью пользуются методики со­ставления оргсхем или организационных чертежей, на которых графически изображается каждое рабочее ме­сто, прописываются должностные обязанности и опре­деляются информационные потоки для отдельного ис­полнителя.

При такой схеме управления и контроля предельно ясно, на каком участке (отдел, служба, управление) требуется специалист соответствующей квалификации и какой информацией он должен располагать для вы­полнения функций на своем рабочем месте. Внутрен­ними распоряжениями также определяются требова­ния к деловым и личным качествам сотрудников и обусловливаются режимы сохранения или коммерчес­кой тайны.

Кроме того, для большей конкретизации этих про­цедур на каждое рабочее место рекомендуется состав­лять профессиограмму, т.е. перечень личностных ка­честв, которыми в идеале должен обладать потенциаль­ный сотрудник. Содержательная сторона и глубина проработки профессиограмм могут быть различными. Это зависит в первую очередь от того, на какое рабо­чее место они составляются.

Однако обязательными атрибутами подобных до­кументов являются разделы, отражающие профессио­нально значимые качества (психологические характери­стики, свойства личности, без которых невозможно выполнение основных функциональных обязанностей), а также противопоказания (личностные качества, кото­рые делают невозможным зачисление кандидата на кон­кретную должность). В некоторых случаях необходимо не только указывать профессионально значимые каче­ства, но и оценивать степень их выраженности, т.е. сформированности.

После разработки схем управления и составления профессиограмм можно приступать к собеседованиям и применять разнообразные процедуры отбора кан­дидатов на работу. Как правило, проблема отбора кадров встает перед руководителями банков в двух основных случаях: создание новых подразделений, замещение вакантных должностей. Для первого случая характерно, как правило, изуче­ние значительного числа кандидатур, для которых из набора имеющихся вакансий подбирается соответст­вующая должность. Во втором случае из ограничен­ного числа кандидатов отбирается тот, который по своим личным и профессиональным качествам в на­ибольшей степени соответствует требованиям профессиограммы данного рабочего места.

Проблема состоит в том, что даже весьма опыт­ные работники кадровых подразделений не всегда мо­гут правильно, достоверно и быстро оценить подлин­ное психическое состояние лиц, пришедших на собеседо­вание. Этому способствуют повышенное волнение, склонность отдельных кандидатов к предвзятым оцен­кам характера деятельности некоторых коммерческих структур, но особенно широкое и зачастую бесконт­рольное самолечение различных психосоматических расстройств с использованием в ряде случаев весьма сильных психотропных препаратов. В этой связи веду­щие московские коммерческие банки требуют от кан­дидатов предоставления справок о состоянии здоровья либо сами выдают направления в определенные поликлиники с рекомендацией прохождения полной диспан­серизации (за счет кандидата).

С точки зрения обеспечения страте­гических интересов коммерческой структуры **являются обязательными следующие функции службы безопас­ности:**

- определение степени вероятности формирования у кандидата преступных наклонностей в случаях воз­никновения в его окружении определенных благопри­ятных обстоятельств (персональное распоряжение кре­дитно-финансовыми ресурсами, возможность контро­ля за движением наличных средств и ценных бумаг, доступ к материально-техническим ценностям, работа с конфиденциальной информацией и пр.);

- выявление имевших место ранее преступных на­клонностей, судимостей, связей с криминальной сре­дой (преступное прошлое, наличие конкретных суди­мостей, случаи афер, махинаций, мошенничества, хи­щений на предыдущем месте работы кандидата и уста­новление либо обоснованное суждение о его возмож­ной причастности к этим преступным деяниям).

Для добывания подобной информации использу­ются возможности различных подразделений банковских структур, в первую очередь службы безопасности, отдела кадров, юридического отдела, под­разделений медицинского обеспечения, а также не­которых сторонних организаций, например, детек­тивных агентств, бюро по занятости населения, диспансеров и пр.

Очевидно также, что представители банковских структур должны быть абсолютно уверены в том, что проводят тесты, собеседования и встречи именно с те­ми лицами, которые выступают в качестве кандидатов на работу. Это подразумевает тщательную проверку паспортных данных, иных документов, а также получе­ние **фотографий кандидатов без очков, контактных линз, парика, макияжа.**

Рекомендуется настаивать на получении набора цветных фотографий кандидата, которые могут быть использованы в случае необходимости для предъявле­ния жильцам по месту его проживания или коллегам по работе. Использование в кадровой работе цветных фотографий, соответствующих паспортным данным, предпочтительнее также в связи с тем, что они четко и без искажений передают цвет волос, глаз, кожи, возраст и характерные приметы кандидата.

В практике уже известны случаи, когда для допол­нительного анализа анкеты кандидата и его фотогра­фий руководители банковских структур приглашали высокопрофессиональных юристов, графологов, из­вестных психоаналитиков с целью обеспечения максимальной полноты формулировок окончательного заключения и выявления возможных скрытых противоречий в характере проверяемого лица.

В том случае, если результаты указанных проверок, тестов и психологического изучения не противоречат друг другу и не содержат данных, которые бы препят­ствовали приему на работу данного кандидата, с ним заключается трудовое соглашение, в большинстве слу­чаев предусматривающее определенный испытатель­ный срок (1-3 месяца).

Необходимо также подчеркнуть следующее важное обстоятельство - лица, принима­емые на ответственные вакантные должности в ком­мерческих структурах (члены правлений, главные бух­галтеры, консультанты, начальники служб безопасно­сти и охраны, руководители компьютерных центров и цехов, помощники и секретари первых лиц) сегодня подвергаются, как правило, следующей стандартной проверке, включающей:

• достаточно продолжительные процедуры сбора и верификации установочно-  
биографических сведений с их последующей аналитической обработкой;

• предоставление рекомендательных писем от известных  
предпринимательских структур с их последующей проверкой;

• проверки по учетам правоохранительных органов; установки по месту  
жительства и по предыдущим местам работы;

• серии собеседований и тестов с последующей психоаналитической  
обработкой результатов.

По мнению экспертов, даже каждый, взятый в от­дельности из упомянутых методов проверки доста­точно эффективен. В совокупности же достигается весьма высокая степень достоверности информации о профессиональной пригодности и надежности ка­ндидата, его способностях к творческой работе на конкретном участке в соответствующем коммерческом предприятии.

Серьезное влияние на **вопросы безопасности** ком­мерческих предприятий оказывают процедуры уволь­нения сотрудников. К сожалению, отдельных руково­дителей порой мало интересуют чувства и пережива­ния персонала, который по тем или иным причинам попадает под сокращение или самостоятельно изъяв­ляет желание покинуть банк или акционерное обще­ство. Как показывает опыт, такой подход приводит, как правило, к серьезным негативным последствиям.

Современные психологические подходы к процессу увольнения позволяют выработать следующую при­нципиальную рекомендацию: каковы бы ни были причи­ны увольнения сотрудника, он должен покидать коммер­ческую организацию **без чувства обиды, раздраже****ния и** **мести.**

Только в этом случае можно надеяться на то, что увольняемый сотрудник не предпримет необдуманных шагов и не проинформирует правоохранительные ор­ганы, налоговую инспекцию, конкурентов, криминаль­ные структуры об известных ему аспектах работы банка. Кроме того, известны случаи мести бывших сотрудников с использованием компьютерного проникновения.

Таким образом, представители кадровых подраз­делений и служб безопасности должны быть четко ориентированы на выяснение истинных мотивов уво­льнения всех категорий сотрудников. Зачастую причи­ны, на которые ссылается сотрудник при увольнении, и подлинные мотивы, побудившие его к такому шагу, существенно отличаются друг от друга. Обычно лож­ный защитный мотив используется потому, что со­трудник в силу прежних привычек и традиций опасает­ся неправильной интерпретации своих действий со сто­роны руководителей и коллег по работе.

Наряду с этим весьма часто имеют место случаи, когда сотрудник внутренне сам уверен в том, что увольняется по откровенно называемой им причине, хотя его решение сформировано и принято под влия­нием совершенно иных, порой скрытых от него обсто­ятельств. Так, в практике уже известны случаи весьма тонких и тайных комбинаций оказания влияния на высококвалифицированных специалистов с целью их переманивания на другое место работы.

В этой связи принципиальная задача состоит в том, чтобы определить истинную причину увольнения со­трудника, попытаться правильно ее оценить и решить, целесообразно ли в данной ситуации предпринимать попытки к искусственному удержанию данного лица в коллективе либо отработать и реализовать процеду­ру его спокойного и бесконфликтного увольнения. Ре­шение рекомендуется принимать на основе строго объективных данных в отношении каждого конкрет­ного сотрудника.

При поступлении устного или письменного заявле­ния об увольнении рекомендуется во всех без исключе­ниях случаях провести с сотрудником беседу с участи­ем представителя кадрового подразделения и кого-ли­бо из руководителей коммерческой структуры. Однако до беседы целесообразно предпринять меры по сбору следующей информации об увольняющемся сотруднике:

- характер его взаимоотношений с коллегами в кол­лективе; отношение к работе; уровень профессиональной подготовки; наличие конфликтов личного или служебного хара­ктера;

- ранее имевшие место высказывания или пожелания перейти на другое место работы;

- доступ к информации, в том числе составляющей коммерческую тайну;

- вероятный период устаревания сведений, составля­ющих коммерческую тайну для данного предприятия; предполагаемое в будущем место работы увольня­ющегося (увольняемого) сотрудника.

Беседа при увольнении проводится лишь только после того, когда собраны все необходимые сведения. Конечно, предварительно руководитель коммерческой структуры отрабатывает принципиальный подход к вопросу о том, целесообразно ли предпринимать попытки склонить сотрудника изменить его первона­чальное решение либо санкционировать оформление его увольнения. В любом случае рекомендуется дать собеседнику высказаться и в развернутой форме объяс­нить мотивы своего решения. При выборе места про­ведения беседы предпочтение отдается, как правило, служебным помещениям.

В зависимости от предполагаемого результата беседа может проводиться в официальном тоне либо иметь форму доверительной беседы, задушевного разговора, обмена мнениями. Однако каковы бы ни были планы в отношении данного сотрудника, раз­говор с ним должен быть построен таким образом, чтобы последний ни в коей мере не испытывал чувства униженности, обиды, оскорбленного достоинства. Для этого следует сохранять тон беседы предельно кор­ректным, тактичным и доброжелательным, даже не­смотря на любые критические и несправедливые заме­чания, которые могут быть высказаны сотрудником в адрес банковской структуры и ее конкретных менеджеров.

Если менеджером банка, отделом кадров и службой безопасности все же принято решение не препятствовать увольнению сотрудника, а по своему служебному положению он располагал доступом к конфиденциальной информации, то в этом случае от­рабатывается несколько вариантов сохранения в тайне коммерческих сведений (оформление официальной подписи о неразглашении данных, составляющих ком­мерческую тайну, либо устная «джентльменская» до­говоренность о сохранении увольняемым сотрудником лояльности к «своему банку или фирме»).

В этой связи необходимо подчеркнуть, что личное обращение к чувству чести и достоинства увольняемых лиц наиболее эффективно в отношении тех индивиду­умов, которые обладают темпераментом сангвиника и флегматика, высоко оценивающих, как правило, до­верие и доброжелательность.

Что касается лиц с темпераментом холерика, то с этой категорией сотрудников рекомендуется завер­шать беседу на официальной ноте. В ряде случаев объявление им принятого решения об увольнении вы­зывает бурную негативную реакцию, связанную с по­пытками спекулировать на своих истинных, а порой и мнимых профессиональных достоинствах. Поэтому с сотрудниками такого темперамента и склада харак­тера целесообразно тщательно оговаривать и обуслов­ливать в документах возможности наступления для них юридических последствий раскрытия коммерчес­кой тайны.

Несколько иначе рекомендуется действовать в тех случаях, когда увольнения сотрудников происходят по инициативе самих коммерческих структур. В этих об­стоятельствах не следует поспешно реализовывать принятое решение. Если увольняемое лицо располага­ет какими-либо сведениями, составляющими коммерческую тайну, то целесообразно предварительно и под соответствующим предлогом перевести его на другой участок работы, например в такое подразделение, в ко­тором отсутствует подобная информация.

Кроме того, таких лиц традиционно стремятся со­хранить в структуре банка или фирмы (их дочерних предприятий, филиалов) до тех пор, пока не будут приняты меры к снижению возможного ущерба от разглашения ими сведений, составляющих коммерчес­кую тайну, либо найдены адекватные средства защиты конфиденциальных данных (технические, администра­тивные, патентные, юридические, финансовые и пр.).

Только лишь после реализации этих мер рекомен­дуется приглашать на собеседование подлежащего уво­льнению сотрудника и объявлять конкретные причи­ны, по которым коммерческая организация отказыва­ется от его услуг. Желательно при этом, чтобы эти причины содержали элементы объективности, достове­рности и проверяемости (перепрофилирование произ­водства, сокращение персонала, ухудшение финансово­го положения, отсутствие заказчиков и пр.). При моти­вации увольнения целесообразно, как правило, воздер­живаться от ссылок на негативные деловые и личные качества данного сотрудника.

После объявления об увольнении рекомендуется внимательно выслушивать контрдоводы, аргументы и замечания сотрудника в отношении характера рабо­ты, стиля руководства компанией и т. п. Обычно уво­льняемый персонал весьма критично, остро и правдиво освещает ситуацию в коммерческих структурах, вскры­вая уязвимые места, серьезные недоработки, кадровые просчеты, финансовые неурядицы и т. п.

Если подходить не предвзято и объективно к подо­бной критике, то эти соображения могут быть исполь­зованы в дальнейшем весьма эффективно в интересах самого банка. В ряде случаев увольняемому со­труднику вполне серьезно предлагают даже изложить письменно свои рекомендации, конечно, за соответст­вующее вознаграждение.

При окончательном расчете обычно рекомендуется независимо от личностных характеристик увольняемых сотрудников брать у них подписку о неразглашении конфиденциальных сведений, ставших известными в процессе работ.

В любом случае после увольнения сотрудников, осведомленных о сведениях, составляющих коммер­ческую тайну, целесообразно через возможности служ­бы безопасности банка или фирмы (частного детектив­ного агентства) проводить оперативную установку по их новому месту работы и моделировать возможности утечки конфиденциальных данных.

Кроме того, в наиболее острых и конфликтных ситуациях увольнения персонала проводятся оператив­ные и профилактические мероприятия по новому месту работы, жительства; также в окружении носителей коммерческих секретов.

Персонал оказывает су­щественное, а в большинстве случаев даже решающее влияние на информационную безопасность банка. В этой связи подбор кадров, их изучение, рас­становка и квалифицированная работа при увольнени­ях в значительной степени повышают устойчивость коммерческих предприятий к возможному стороннему негативному влиянию и агентурному проникновению противоправных элементов.

Регулярное изучение всех категорий персонала, по­нимание объективных потребностей сотрудников, их ведущих интересов, подлинных мотивов поведения и выбор соответствующих методов объединения от­дельных индивидуумов в работоспособный коллек­тив — все это позволяет руководителям в итоге ре­шать сложные производственные и коммерческо-финансовые задачи, в том числе связанные с обеспечением экономической безопасности.

Обобщая основные рекомендации, представляется, что программа работы с персоналом в коммерческой структуре могла бы быть сформулирована следующим образом:

- добывание в рамках действующего российского за­конодательства максимального объема сведений о ка­ндидатах на работу, тщательная проверка представ­ленных документов как через официальные, так и опе­ративные возможности, в том числе службы безопас­ности банка или частного детективного агент­ства, системность в анализе информации, собранной на соответствующие кандидатуры;

- проведение комплекса проверочных мероприятий в отношении кандидатов на работу, их родственников, бывших сослуживцев, ближайшего окружения в тех случаях, когда рассматривается вопрос об их приеме на руководящие должности или допуске к информа­ции, составляющей коммерческую тайну;

- использование современных методов, в частности собеседований и тестирований, для создания психоло­гического портрета кандидатов на работу, который бы позволял уверенно судить об основных чертах харак­тера и прогнозировать их вероятные действия в раз­личных экстремальных ситуациях;

- оценка с использованием современных психологи­ческих методов разноплановых и разнопорядковых фа­кторов, возможно препятствующих приему кандида­тов на работу или их использованию на конкретных должностях;

- определение для кандидатов на работу в коммер­ческих структурах некоторого испытательного срока с целью дальнейшей проверки и выявления деловых и личных качеств, иных факторов, которые бы могли препятствовать зачислению на должность;

- введение в практику регулярных и неожиданных комплексных проверок персонала, в том числе через возможности служб безопасности;

- обучение сотрудников кадровых подразделений и служб безопасности современным психологическим подходам к работе с персоналом, социальным, психо­аналитическим, этико-моральным методам, навыкам использования современных технических средств для фиксирования результатов интервью и собеседований, приемам проведения целевых бесед «втемную» и про­цедурам информационно-аналитической работы с до­кументами кандидатов;

- выделение из числа первых руководителей ком­мерческих структур куратора кадровой работы для осуществления контроля за деятельностью кадровых подразделений и служб безопасности при работе с пе­рсоналом.

Можно сделать определенный вывод о том, что российские предприниматели во все возрастающей степени меняют свое отношение к «человеческому фак­тору», ставят на вооружение своих кадровых подраз­делений и служб безопасности современные методы работы с персоналом. Очевидно, что дальнейшее раз­витие в этой области связано с активным использова­нием значительного потенциала методов психоанали­за, психологии и этики управления, конфликтологии и ряда других наук и более полного интегрирования соответствующих специалистов в коммерческие пред­приятия.

**Безопасность автоматизированных систем обработки информации в банках (АСОИБ).**

Воздействию могут подвергаться следующие компоненты АСОИБ:

а. АСОИБ в целом - злоумышленник пытается проникнуть в систему для последующего выполнения каких-либо несанкционированных действий. Для этого обычно используются метод «маскарада», перехват или подделка пароля, взлом или доступ к АСОИБ через сеть.

б. Объекты АСОИБ - данные или программы в оперативной памяти или на внешних носителях, сами устройства системы, как внешние (дисководы, сетевые устройства, терминалы), так и внутренние (оперативная память, процессор), каналы передачи данных. Воздействие на объекты системы обычно имеет целью доступ к их содержимому (нарушение конфиденциальности или целостности обрабатываемой или хранимой информации) или нарушение их функциональности, например, заполнение всей оперативной памяти компьютера бессмысленной информацией или загрузка процессора компьютера задачей с неограниченным временем исполнения (нарушение доступности АСОИБ).

в. Субъекты АСОИБ — процессы и подпроцессы пользователей. Целью таких атак является либо прямое воздействие на работу процесса — его приостановка, изменение привилегий или характеристик (приоритета, например), либо обратное воздействие — использование злоумышленником привилегий, характеристик и т.д. другого процесса в своих целях. Частным случаем такого воздействия является внедрение злоумышленником вируса в среду другого процесса и его выполнение от имени этого процесса. Воздействие может осуществляться на процессы пользователей, системы, сети.

г. Каналы передачи данных — пакеты данных, передаваемые по каналу связи и сами каналы. Воздействие на пакеты данных может рассматриваться как атака на объекты сети, воздействие на каналы — специфический род атак, характерный для сети. К нему относятся: прослушивание канала и анализ трафика (потока сообщений) — нарушение конфиденциальности передаваемой информации; подмена или модификация сообщений в каналах связи и на узлах ретрансляторах — нарушение целостности передаваемой информации; изменение топологии и характеристик сети, правил коммутации и адресации —нарушение доступности сети.

Для воздействия на систему злоумышленник может использовать стандартное программное обеспечение или специально разработанные программы. В первом случае результаты воздействия обычно предсказуемы, так как большинство стандартных программ АСОИБ хорошо изучены. Использование специально разработанных программ связано с большими трудностями, но может быть более опасным, поэтому в защищенных системах рекомендуется не допускать добавление программ в АСОИБ без разрешения администратора безопасности системы.

Состояние объекта в момент атаки может оказать существенное влияние на результаты атаки и на работу по ликвидации ее последствий. Объект атаки может находиться в одном из трех состояний:

а. Хранения — на диске, магнитной ленте, в оперативной памяти или любом другом месте в пассивном состоянии. При этом воздействие на объект обычно осуществляется с использованием доступа;

б. Передачи — по линии связи между узлами сети или внутри узла. Воздействие предполагает либо доступ к фрагментам передаваемой информации (например, перехват пакетов на ретрансляторе сети), либо просто прослушивание с использованием скрытых каналов;

в. Обработки — в тех ситуациях, когда объектом атаки является процесс пользователя.

Подобная классификация показывает сложность определения возможных угроз и способов их реализации. Это еще раз подтверждает тезис, что определить все множество угроз АСОИБ и способов их реализации не представляется возможным. Не существует универсального способа защиты, который предотвратил бы любую угрозу. Этот факт обуславливает необходимость объединения различных мер защиты для обеспечения безопасности всей АСОИБ в целом.

Выше была рассмотрена классификация возможных угроз безопасности АСОИБ. Конечно, не все приведенные классы угроз являются независимыми от остальных, не для любой угрозы можно определить, к какому виду в каждом из перечисленных классов она принадлежит. Приведенная выше классификация охватывает большинство основных угроз безопасности АСОИБ, которые должны найти свое место в одном или нескольких выделенных классах.

Далее приведено более подробное описание угроз, с которыми наиболее часто приходится сталкиваться администраторам безопасности.

**Несанкционированный доступ** (НСД).

Это наиболее распространенный вид компьютерных нарушений. Он заключается в получении пользователем доступа к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности. Обычно самая главная проблема определить, кто и к каким наборам данных должен иметь доступ, а кто нет. Другими словами, необходимо определить термин «несанкционированный».

По характеру воздействия НСД является активным воздействием, использующим ошибки системы. НСД обращается обычно непосредственно к требуемому набору данных, либо воздействует на информацию о санкционированном доступе с целью легализации НСД. НСД может быть подвержен любой объект системы. НСД может быть осуществлен как стандартными, так и специально разработанными программными средствами к объектам в любом состоянии.

Методика реализации НСД в значительной мере зависит от организации обработки информации в АСОИБ, разработанной для АСОИБ политики безопасности, возможностей установленных средств защиты, а также добросовестности администратора и оператора. Для реализации НСД существует два способа:

- во-первых, можно преодолеть систему защиты, то есть путем различных воздействий на нее прекратить ее действия в отношении себя или своих программ. Это сложно, трудоемко и не всегда возможно, зато эффективно;

- во-вторых, можно понаблюдать за тем, что «плохо лежит», то есть какие наборы данных, представляющие интерес для злоумышленника, открыты для доступа по недосмотру или умыслу администратора. Такой доступ, хотя и с некоторой натяжкой, тоже можно назвать несанкционированным, его легко осуществить, но от него легко и защититься. К этому же типу относится НСД с подбором пароля, поскольку осуществить такой подбор возможно лишь в случае нарушения правил составления паролей и использования в качестве пароля человеческих имен, повторяющихся символов, наборов типа QWERTY.

В подавляющем большинстве случаев НСД становится возможным из-за непродуманного выбора средств защиты, их некорректной установки и настройки, плохого контроля работы, а также при небрежном отношении к защите своих собственных данных.

**Незаконное использование привилегий.**

Злоумышленники, применяющие данный способ атаки, обычно используют штатное программное обеспечение (системное или прикладное), функционирующее в нештатном режиме. Практически любая защищенная система содержит средства, используемые в чрезвычайных ситуациях, при сбоях оборудования или средства, которые способны функционировать с нарушением существующей политики безопасности. В некоторых случаях пользователь должен иметь возможность доступа ко всем наборам системы (например, при внезапной проверке).

Такие средства необходимы, но они могут быть чрезвычайно опасными. Обычно эти средства используются администраторами, операторами, системными программистами и другими пользователями, выполняющими специальные функции.

Для того, чтобы уменьшить риск от применения таких средств большинство систем защиты реализует такие функции с помощью набора привилегий — для выполнения определенной функции требуется определенная привилегия. В этом случае каждый пользователь получает свой набор привилегий, обычные пользователи — минимальный, администраторы — максимальный (в соответствии с принципом минимума привилегий). Наборы привилегий каждого пользователя являются его атрибутами и охраняются системой защиты. Несанкционированный захват привилегий приведет, таким образом, к возможности несанкционированного выполнения определенной функции. Это может быть НСД (частный случай), запуск определенных программ и даже реконфигурация системы.

Естественно, при таких условиях расширенный набор привилегий -заветная мечта любого злоумышленника. Он позволит ему совершать практически любые действия, причем, возможно, даже в обход всех мер контроля. Нарушения, совершаемые с помощью незаконного использования привилегий, являются активным воздействием, совершаемым с целью доступа к какому-либо объекту или системе в целом.

Незаконный захват привилегий возможен либо при наличии ошибок в самой системе защиты (что, например, оказалось возможным в одной из версий операционной системы UNIX), либо в случае халатности при управлении системой и привилегиями в частности (например, при назначении расширенного набора привилегий всем подряд). Строгое соблюдение правил управления системой защиты, соблюдение принципа минимума привилегий позволят избежать таких нарушений.

**Атаки «салями».**

Атаки «салями» более всего характерны для систем, обрабатывающих денежные счета и, следовательно, для банков особенно актуальны. Принцип атак «салями» построен на том факте, что при обработке счетов используются целые единицы (центы, рубли, копейки), а при исчислении процентов нередко получаются дробные суммы.

Например, 6.5% годовых от $102.87 за 31 день составит $0.5495726. Банковская система может округлить эту сумму до $0.55. Однако если пользователь имеет доступ к банковским счетам или программам их обработки, он может округлить ее в другую сторону — до $0.54, а разницу в 1 цент записать на свой счет. Владелец счета вряд ли ее заметит, а если и обратит внимание, то спишет ее на погрешности обработки и не придаст значения. Злоумышленник же получит прибыль в один цент, при обработке 10.000 счетов в день (а в некоторых банках и больше). Его прибыль таким образом составит $1000, т.е. около $300 000 в год.

Отсюда и происходит название таких атак — как колбаса салями изготавливается из небольших частей разных сортов мяса, так и счет злоумышленника пополняется за счет различных вкладчиков. Естественно, такие атаки имеют смысл лишь в тех организациях, где осуществляется не менее 5.000 - 10.000 транзакций в день, иначе не имеет смысла рисковать, поскольку в случае обнаружения преступника просто определить. Таким образом, атаки «салями» опасны в основном для крупных банков.

Причинами атак «салями» являются, во-первых, погрешности вычислений, позволяющие трактовать правила округления в ту или иную сторону, а во-вторых, огромные объемы вычислений, необходимые для обработки счетов. Успех таких атак зависит не столько от величины обрабатываемых сумм, сколько от количества счетов (для любого счета погрешность обработки одинакова). Атаки «салями» достаточно трудно распознаются, если только злоумышленник не начинает накапливать на одном счете миллионы. Предотвратить такие атаки можно только обеспечением целостности и корректности прикладных программ, обрабатывающих счета, разграничением доступа пользователей АСОИБ к счетам, а также постоянным контролем счетов на предмет утечки сумм.

**«Скрытые каналы»**

«Скрытые каналы» - пути передачи информации между процессами системы, нарушающие системную политику безопасности. В среде с разделением доступа к информации пользователь может не получить разрешение на обработку интересующих его данных, однако может придумать для этого обходные пути. Практически любое действие в системе каким-то образом затрагивает другие ее элементы, которые при этом могут изменять свое состояние. При достаточной наблюдательности и знании этих связей можно получить прямой или опосредованный доступ к данным.

«Скрытые каналы» могут быть реализованы различными путями, в частности при помощи программных закладок («троянских коней»).

Например, программист банка не всегда имеет доступ к именам и балансам депозитных счетов. Программист системы, предназначенной для обработки ценных бумаг, может не иметь доступ к предложениям о покупке или продаже. Однако при создании таких систем он может предусмотреть способ получения интересующих его сведений. В этом случае программа скрытым способом устанавливает канал связи с этим программистом и сообщает ему требуемые сведения.

Атаки с использованием скрытых каналов обычно приводят к нарушениям конфиденциальности информации в АСОИБ, по характеру воздействия являются пассивными: нарушение состоит только в передаче информации. Для организации «скрытых каналов» может использоваться как штатное программное обеспечение, так и специально разработанные «троянские» или вирусные программы. Атака обычно производится программным способом.

Примером передачи информации по «скрытым каналам» может служить, например, итоговый отчет, в котором вместо слова «TOTAL» используется слово «TOTALS» - программист сделал так, что при определенных условиях, которые может распознать его программа, должна происходить замена слов. Подобными «скрытыми каналами» могут стать число пробелов между двумя словами, значение третьей или четвертой цифры после запятой в какой-нибудь дроби (на которые никто не обращает внимания) и т.д. «Скрытым каналом» может явиться и передача информации о наличии или отсутствии какого-либо набора данных, его размере, дате создания или модификации и т.д.

Также существует большое количество способов организации связи между двумя процессами системы. Более того, многие операционные системы имеют в своем распоряжении такие средства, так как они очень облегчают работу программистов и пользователей. Проблема заключается в том, что очень трудно отделить неразрешенные «скрытые каналы» от разрешенных, то есть тех, которые не запрещаются системной политикой безопасности. В конечном счете все определяется ущербом, который может принести организация «скрытых каналов».

Отличительными особенностями «скрытых каналов» является их малая пропускная способность (по ним обычно можно передавать только небольшое количество информации), большие трудности их организации и обычно небольшой наносимый ими ущерб. Более того, он вообще бывает незаметен, поэтому специальные меры защиты против «скрытых каналов» предпринимают довольно редко. Обычно достаточно грамотно разработанной полномочной политики безопасности.

**«Маскарад».**

Под «маскарадом» понимается выполнение каких-либо действий одним пользователем АСОИБ от имени другого пользователя. При этом такие действия другому пользователю могут быть разрешены. Нарушение заключается в присвоении прав и привилегий.

Такие нарушения также называются симуляцией или моделированием. Цель «маскарада» — сокрытие каких-либо действий за именем другого пользователя или присвоение прав и привилегий другого пользователя для доступа к его наборам данных или для использования его привилегий.

«Маскарад» — это способ активного нарушения защиты системы, он является опосредованным воздействием, то есть воздействием, совершенным с использованием возможностей других пользователей.

Примером «маскарада» может служить вход в систему под именем и паролем другого пользователя, при этом система защиты не сможет распознать нарушение. В этом случае «маскараду» обычно предшествует взлом системы или перехват пароля.

Другой пример «маскарада» — присвоение имени другого пользователя в процессе работы. Это может быть сделано с помощью средств операционной системы (некоторые операционные системы позволяют изменять идентификатор пользователя в процессе работы) или с помощью программы, которая в определенном месте может изменить определенные данные, в результате чего пользователь получит другое имя. В этом случае «маскараду» может предшествовать захват привилегий, или он может быть осуществлен с использованием какой-либо ошибки в системе.

«Маскарадом» также называют передачу сообщений в сети от имени другого пользователя. Способы замены идентификатора могут быть разные, обычно они определяются ошибками и особенностями сетевых протоколов. Тем не менее на приемном узле такое сообщение будет воспринято как корректное, что может привести к серьезным нарушениям работы сети. Особенно это касается управляющих сообщений, изменяющих конфигурацию сети, или сообщений, ведущих к выполнению привилегированных операций. [8]

Наиболее опасен «маскарад» в банковских системах электронных платежей, где неправильная идентификация клиента может привести к огромным убыткам. Особенно это касается платежей с помощью электронных банковских карт. Сам по себе метод идентификации с помощью персонального идентификатора (PIN) достаточно надежен, нарушения могут происходить вследствие ошибок его использования. Это произойдет, например, в случае утери кредитной карты, при использовании очевидного идентификатора (своего имени, ключевого слова и т.д.). Поэтому клиентам надо строго соблюдать все рекомендации банка по выполнению такого рода платежей.

«Маскарад» является достаточно серьезным нарушением, которое может привести к тяжелым последствиям, таким как изменение конфигурации системы (сети), утечка информации, нарушения работы АСОИБ. Для предотвращения «маскарада» необходимо использовать надежные методы идентификации и аутентификации, блокировку попыток взлома системы, контроль входов в нее. Также необходимо фиксировать все события, которые могут свидетельствовать о «маскараде», в системном журнале для его последующего анализа.

**«Сборка мусора».**

После окончания работы обрабатываемая информация не всегда полностью удаляется из памяти. Часть данных может оставаться в оперативной памяти, на дисках и лентах, других носителях. Данные хранятся на носителе до перезаписи или уничтожения; при выполнении этих действий на освободившемся пространстве диска находятся их остатки. Хотя прочитать такие данные трудно, однако, используя специальные программы и оборудование, все же возможно. Такой процесс принято называть «сборкой мусора». Он может привести к утечке важной информации.

«Сборка мусора» — активное, непосредственное воздействие на объекты АСОИБ при их хранении с использованием доступа. Это воздействие может привести к нарушению конфиденциальности информации.

Для защиты от «сборки мусора» используются специальные механизмы, которые могут быть реализованы в операционной системе и/или аппаратуре компьютера или в дополнительных программных (аппаратных) средствах. Примерами таких механизмов являются стирающий образец и метка полноты:

- стирающий образец — это некоторая последовательность битов, записываемая на место, освобождаемое файлом. Менеджер или администратор безопасности АСОИБ может автоматически активизировать запись этой последовательности при каждом освобождении участка памяти, при этом стираемые данные уничтожаются физически.

- метка полноты предотвращает чтение участков памяти, отведенных процессу для записи, но не использованных им. Верхняя граница адресов использованной памяти и есть метка полноты. Этот способ используется для защиты последовательных файлов исключительного доступа (результирующие файлы редакторов, компиляторов, компоновщиков т.д.). Для индексных и разделяемых последовательных файлов этот метод называется «стирание при размещении», память очищается при выделении ее процессу.

**«Взлом системы».**

Под «взломом системы» понимают умышленное проникновение в систему с несанкционированными параметрами входа, то есть именем пользователя и его паролем (паролями).

«Взлом системы» — умышленное, активное воздействие на систему в целом. «Взлом системы» обычно происходит в интерактивном режиме.

Поскольку имя пользователя не является секретом, объектом «охоты» обычно становится пароль. Способы вскрытия пароля могут быть различны: перебор возможных паролей, «маскарад» с использованием пароля другого пользователя, захват привилегий. Кроме того, «взлом системы» можно осуществить, используя ошибки программы входа.

Таким образом, основную нагрузку на защиту системы от «взлома» несет программа входа. Алгоритм ввода имени и пароля, их шифрование (при необходимости), правила хранения и смены паролей не должны содержать ошибок. Противостоять «взлому системы» также поможет например, ограничение количества попыток неправильного ввода пароля с последующей блокировкой терминала и уведомлением оператора в случае нарушения.

Кроме того, оператор должен постоянно контролировать активных пользователей системы: их имена, характер работы, время входа и выхода и т.д. Такие действия помогут своевременно установить факт «взлома» и позволят предпринять необходимые действия.

**«Люки».**

«Люк» — это скрытая, недокументированная точка входа в программный модуль. «Люк» вставляется в программу обычно на этапе отладки для облегчения работы: программный модуль можно вызывать в разных местах, что позволяет отлаживать отдельные его части независимо. Но в дальнейшем программист может забыть уничтожить «люк» или некорректно его заблокировать. Кроме того, «люк» может вставляться на этапе разработки для последующей связи данного модуля с другими модулями системы, но затем, в результате изменившихся условий данная точка входа оказывается ненужной.

Наличие «люка» позволяет вызывать программу нестандартным образом, что может серьезно сказаться на состоянии системы защиты (неизвестно, как в таком случае программа будет воспринимать данные, среду системы и т.д.). Кроме того, в таких ситуациях не всегда можно прогнозировать ее поведение.

«Люк» относится к категории угроз, возникающих вследствие ошибок реализации какого-либо проекта (АСОИБ в целом, комплекса программ и т.д.). Поскольку использование «люков» может быть самым разным и зависит от самой программы, классифицировать данную угрозу как-либо еще затруднительно.

«Люки» могут оказаться в программах по следующим причинам:

- их забыли убрать;

- для использования при дальнейшей отладке;

- для обеспечения поддержки готовой программы;

- для реализации тайного контроля доступа к данной программе после ее установки.

Первый из перечисленных случаев — ненамеренный промах, который может привести к бреши в системе защиты. Два следующих случая — серьезные испытания для системы безопасности, с которыми она может и не справиться. Четвертый случай может стать первым шагом преднамеренного проникновения с использованием данной программы.

Отметим, что программная ошибка «люком» не является. «Люк» — это достаточно широко используемый механизм отладки, корректировки и поддержки программ, который создается преднамеренно, хотя чаще всего и без злого умысла. Люк становится опасным, если он не замечен, оставлен и не предпринималось никаких мер по контролю за ним.

Большая опасность «люков», особенно в программах операционной системы, компенсируется высокой сложностью их обнаружения. Если не знать заранее, что данная программа содержит «люк», необходимо обработать килобайты (а иногда и мегабайты) программного кода, чтобы найти его. Понятно, что почти всегда это нереально. Поэтому в большинстве случаев обнаружение «люков» — результат случайного поиска. Защита от них может быть только одна — не допускать появления «люков» в программе, а при приемке программных продуктов, разработанных третьими производителями — проводить анализ исходных текстов программ с целью обнаружения «люков».

**Вредоносные программы.**

В последнее время участились случаи воздействия на вычислительную систему при помощи специально созданных программ. Под вредоносными программами в дальнейшем будем понимать такие программы, которые прямо или косвенно дезорганизуют процесс обработки информации или способствуют утечке или искажению информации.

Ниже рассмотрим некоторые (самые распространенные) виды подобных программ: «троянский конь», вирус, «червь», «жадная» про грамма, «захватчик паролей»:

**«Троянский кoнь»** — программа, выполняющая в дополнение к основным (проектным и документированным) не описанные в документации действия. Аналогия с древнегреческим «троянским конем» таким образом вполне оправдана — в не вызывающей подозрений оболочке таится угроза. Программы такого типа являются серьезной угрозой безопасности АСОИБ.

По характеру угрозы «троянский конь» относится к активным угрозам, реализуемым программными средствами, работающими в пакетном режиме. Он может угрожать любому объекту АСОИБ. Наиболее опасным является опосредованное воздействие, при котором «троянский конь» действует в рамках полномочий одного пользователя, но в интересах другого пользователя, установить личность которого порой невозможно.

Опасность «троянского коня» заключается в дополнительном блоке команд, тем или иным образом вставленном в исходную безвредную программу, которая затем предлагается (дарится, продается, подменяется) пользователям АСОИБ. Этот блок команд может срабатывать при наступлении некоторого условия (даты, времени и т.д., либо по команде извне). Запустивший такую программу подвергает опасности как себя и свой файлы, так и всю АСОИБ в целом.

Наиболее опасные действия «троянский конь» может выполнять, если запустивший ее пользователь обладает расширенным набором привилегий. В этом случае злоумышленник, составивший и внедривший «троянского коня», и сам этими привилегиями не обладающий, может выполнить несанкционированные привилегированные функции чужими руками. Или, например, злоумышленника очень интересуют наборы данных пользователя, запустившего такую программу. Последний может даже не обладать расширенным набором привилегий — это не помешает выполнению несанкционированных действий.

Характерным примером «Троянского коня» является появившийся в Интернете в январе 1999 г. бесплатно распространяемый Screen Saver, который помимо вывода красивых картинок на экране, осуществляет поиск на компьютере программы-шифровальщика алгоритма DEC. В случае обнаружения программы, Screen Saver ставит под контроль обмен ключами шифрования и пересылает ключи по электронной почте на анонимный сервер в Китае. [17]

«Троянский конь» — одна из наиболее опасных угроз безопасности АСОИБ. Радикальным способом защиты от этой угрозы является создание замкнутой среды исполнения программ. В особенности важно разделение внешних сетей (особенно Интернет) и внутренних сетей по крайней мере на уровне протоколов, а еще лучше — на физическом уровне. Желательно также, чтобы привилегированные и непривилегированные пользователи работали с разными экземплярами прикладных программ, которые должны храниться и защищаться индивидуально. При соблюдении этих мер вероятность внедрения программ подобного рода будет достаточно низкой.

**Вирус** — это программа, которая может заражать другие программы путем включения в них своей, возможно модифицированной, копии, причем последняя сохраняет способность к дальнейшему размножению. Вирус может быть охарактеризован двумя основными особенностями :

- способностью к самовоспроизведению. Это свойство означает, что за время своего существования на компьютере вирус должен хотя бы один раз воспроизвести свою копию на долговременном носителе;

- способностью к вмешательству (получению управления) в вычислительный процесс. Это свойство является аналогом «паразитирования» в живой природе, которое свойственно биологическим вирусам.

Как и «троянские кони» вирусы относятся к активным программным средствам. Классификация вирусов, используемые ими методы заражения, способы борьбы с ними достаточно хорошо изучены и описаны. Эта проблема в нашей стране стала особенно актуальной, поэтому очень многие занимаются ею.

Проблема защиты от вирусов может рассматриваться с двух сторон: как самостоятельная проблема и как одна из сторон проблемы общей защиты АСОИБ. И тот, и другой подходы имеют свои отличительные особенности и, соответственно, свои собственные методы решения проблемы.

В последнее время удалось более или менее ограничить масштабы заражений и разрушений. Тут сыграли свою роль и превентивные меры, и новые антивирусные средства, и пропаганда всех этих мер.

Вообще говоря проблема вирусов может стать тем толчком, который приведет к новому осмыслению как концепций защиты, так и принципов автоматизированной обработки информации в целом.

«**Червь**» — программа, распространяющаяся через сеть и (в отличие от вируса) не оставляющая своей копии на магнитном носителе. «Червь» использует механизмы поддержки сети для определения узла, который может быть заражен. Затем с помощью тех же механизмов передает свое тело или его часть на этот узел и либо активизируется, либо ждет для этого подходящих условий.

Наиболее известный представитель этого класса - вирус Морриса (или, вернее, «червь Морриса»), поразивший сеть Internet в 1988 г. Наиболее подходящей средой распространения «червя» является сеть, все пользователи которой считаются дружественными и доверяют друг другу. Отсутствие защитных механизмов как нельзя лучше способствует уязвимости сети.

Самый лучший способ защиты от «червя» — принять меры предосторожности против несанкционированного доступа к сети.

Таким образом, как вирусы, так «троянские кони» и «черви» на сегодняшний день являются одной из самых опасных угроз АСОИБ. Для защиты от этих разновидностей вредоносных программ необходимо создание замкнутой среды исполнения программ, разграничение доступа к исполняемым файлам, контроль целостности исполняемых файлов и системных областей, тестирование приобретаемых программных средств.

«Жадные» программы — это программы, которые при выполнении стремятся монополизировать какой-либо ресурс системы, не давая другим программам возможности использовать его. Доступ таких программ к ресурсам системы обычно приводит к нарушению ее доступности. Естественно, такая атака будет активным вмешательством в работу системы. Непосредственной атаке обычно подвергаются ключевые объекты системы: процессор, оперативная память, устройства ввода-вывода.

Многие компьютеры, особенно в исследовательских центрах, имеют фоновые программы, выполняющиеся с низким приоритетом. Они обычно производят большой объем вычислений, а результаты их работы требуются не так часто. Однако при повышении приоритета такая программа может блокировать все остальные. Такая программа и будет «жадной».

Тупиковая ситуация возникает, когда «жадная» программа бесконечна (например, исполняет заведомо бесконечный цикл). Однако во многих операционных системах существует возможность ограничения времени процессора, используемого задачей. Это не относится к операциям, выполняющимся в зависимости от других программ, например, к операциям ввода-вывода, которые завершаются асинхронно к основной программе; время их выполнения не включается в счет времени программы. Перехватывая асинхронное сообщение о завершении операции ввода-вывода и посылая вновь запрос на новый ввод-вывод, можно добиться по-настоящему бесконечной программы. Такие атаки называют также асинхронными.

Другой пример «жадной» программы — программа, захватывающая слишком большую область оперативной памяти. В оперативной памяти последовательно размещаются данные, например подкачиваемые с внешнего носителя. В конце концов память может оказаться во владении одной программы, и выполнение других окажется невозможным.

Обычно «жадные» программы осуществляют захват одного из трех основных ресурсов системы: времени процессора, оперативной памяти, каналов ввода-вывода. Однако возможен захват и любых других ресурсов системы: блокирование ее работы, или же использование побочного результата деятельности какой-либо программы (например, вируса). Бороться с захватом ресурсов можно путем введения различных ограничений для выполняемых программ (на время процессора, на количество операций ввода-вывода, на разрешенный объем оперативной памяти и т.д.), а также постоянным операторским контролем за их соблюдением.

**Захватчики паролей**. Это программы специально предназначены для воровства паролей. При попытке входа имитируется ввод имени и пароля, которые пересылаются владельцу программы-захватчика, после чего выводится сообщение об ошибке ввода и управление возвращается операционной системе. Пользователь, думающий, что допустил ошибку при наборе пароля, повторяет вход и получает доступ к системе. Однако его имя и пароль уже известны владельцу программы-захватчика. Перехват пароля может осуществляться и другим способом - с помощью воздействия на программу, управляющую входом пользователей в систему и ее наборы данных.

Для предотвращения этой угрозы перед входом в систему необходимо убедиться, что вы вводите имя и пароль именно системной программе входа, а не какой-то другой. Кроме того, необходимо неукоснительно придерживаться правил использования паролей и работы с системой. Большинство нарушений происходят не из-за хитроумных атак, а из-за элементарной небрежности. Не рекомендуется покидать рабочее место, не выйдя из системы. Постоянно проверяйте сообщения о дате и времени последнего входа и количестве ошибочных входов. Эти простые действия помогут избежать захвата пароля.

Кроме описанных выше, существуют и другие возможности компрометации пароля. Не следует записывать команды, содержащие пароль, в командные процедуры, надо избегать явного объявления пароля при запросе доступа по сети: эти ситуации можно отследить и захватить пароль. Не стоит использовать один и тот же пароль для доступа к разным узлам.

Соблюдение правил использования паролей — необходимое условие надежной защиты.

**Анализ состояния банковских автоматизированных систем с точки зрения безопасности.**

Приведем некоторые **методы оценки вероятностей проявления угроз.**

1. Эмпирическая оценка количества проявлений угрозы за некоторый период времени. Как правило, этот метод применяется для оценки вероятности стихийных бедствий. Невозможно предсказать возникновение, например, пожара в определенном здании, поэтому в таких случаях целесообразно накапливать массив данных об исследуемом событии. Так например, в среднем за год пожар уничтожит некоторое количество зданий; средний ущерб составит $Х. Кроме того, также можно получать данные об обманах со стороны сотрудников, коррупции и т.д. Такой анализ обычно неточен, поскольку использует лишь частичные данные о событии, но тем не менее в некоторых случаях таким путем можно получить приемлемые результаты.

2. Непосредственная регистрация событий. Обычно этот метод применяется для оценки вероятности часто проявляющихся событий (попытки входа в систему, доступ к определенному объекту и т.д.).

3. Оценка частоты проявления угрозы по таблице. Некоторые методы анализа риска позволяют оценить вероятность появления каких либо событий по специальной таблице, выбирая один из коэффициентов. Полнота анализа зависит от качества метода вычисления коэффициентов проявления данного события. Таким образом, оценка вероятности события производится не с помощью безосновательного выбора числа, а на основе системы коэффициентов, которая имеют некоторую методологическую основу.

4. Метод «Дельфийский оракул». С помощью этого метода каждый конкретный коэффициент выводится из частоты появления определенного события. Эти частоты накапливаются и преобразуются в коэффициенты; они могут быть изменены на основе новых данных. После серии испытаний все значения коэффициентов собирают, и если они приемлемы, то одно из них (лучшее в смысле некоторого выбранного критерия) оставляют. В противном случае анализируется методика получения оценок и производится новая серия испытаний.

Определение потерь в результате реализации любой из угроз безопасности — следующий этап анализа риска. Как и оценка частоты реализации различных угроз, определение потерь также трудно поддается расчету. Например, стоимость замены аппаратного или программного обеспечения АСОИБ оценивается достаточно просто. Однако существует много случаев (восстановление данных или программ), когда это сопряжено с большими трудностями.

Многие данные нуждаются в защите по вполне объяснимым причинам. Защищать необходимо личные данные (счета, страховые полисы), коммерческую информацию (технологические, финансовые и другие секреты). Однако при этом трудно оценить величину потерь при искажении, потере этих данных, либо при невозможности получить данные в требуемое время.

**Построение защиты банковских автоматизированных систем.**

Каждую систему обработки информации защиты следует разрабатывать индивидуально учитывая следующие особенности:

* организационную структуру банка;
* объем и характер информационных потоков (внутри банка в целом, внутри отделов, между отделами, внешних);
* количество и характер выполняемых операций: аналитических и повседневных (один из ключевых показателей активности банка — число банковских операций в день, является основой для определения параметров системы);
* количество и функциональные обязанности персонала;
* количество и характер клиентов;
* график суточной нагрузки.

Защита АСОИБ должна разрабатываться для каждой системы индивидуально, но в соответствии с общими правилами. **Построение защиты предполагает следующие этапы:**

- анализ риска, заканчивающийся разработкой проекта системы защиты и планов защиты, непрерывной работы и восстановления;

- реализация системы защиты на основе результатов анализа риска;

- постоянный контроль за работой системы защиты и АСОИБ в целом (программный, системный и административный).

На каждом этапе реализуются определенные требования к защите; их точное соблюдение приводит к созданию безопасной системы.

На сегодняшний день защита АСОИБ — это самостоятельное направление исследований. Поэтому легче и дешевле использовать для выполнения работ по защите специалистов, чем дважды учить своих людей (сначала их будут учить преподаватели, а потом они будут учиться на своих ошибках).

Главное при защите АСОИБ специалистами (естественно после уверенности в их компетенции в данном вопросе) — наличие здравого смысла у администрации системы. Обычно, профессионалы склонны преувеличивать реальность угроз безопасности АСОИБ и не обращать внимания на такие «несущественные детали» как удобство ее эксплуатации, гибкость управления системой защиты и т.д., без чего применение системы защиты становится трудным делом. **Построение системы защиты — это процесс поиска компромисса между уровнем защищенности АСОИБ и сохранением возможности работы в ней.** Здравый смысл помогает преодолеть большинство препятствий на этом пути.

Для обеспечения непрерывной защиты информации в АСОИБ целесообразно создать из специалистов группу информационной безопасности. На эту группу возлагаются обязанности по сопровождению системы защиты, ведения реквизитов защиты, обнаружения и расследования нарушений политики безопасности и т.д.

Один из самых важных прикладных аспектов теории защиты — защита сети. При этом, с одной стороны, сеть должна восприниматься как единая система и, следовательно, ее защита также должна строиться по единому плану. С другой стороны, каждый узел сети должен быть защищен индивидуально.

Защита конкретной сети должна строиться с учетом конкретных особенностей: назначения, топологии, особенностей конфигурации, потоков информации, количества пользователей, режима работы и т.д.

Кроме того, существуют специфические особенности защиты информации на микрокомпьютерах, в базах данных. Нельзя также упускать из виду такие аспекты, как физическая защита компьютеров, периферийных устройств, дисплейных и машинных залов. Иногда бывает необходим и «экзотический» вид защиты — от электромагнитного излучения или защита каналов связи.

**Основные этапы построения системы защиты** заключаются в следующем:

Анализ -> Разработка системы защиты (планирование) -> Реализация системы защиты -> Сопровождение системы защиты.

Этап анализа возможных угроз АСОИБ необходим для фиксирования на определенный момент времени состояния АСОИБ (конфигурации аппаратных и программных средств, технологии обработки информации) и определения возможных воздействий на каждый компонент системы. Обеспечить защиту АСОИБ от всех воздействий на нее невозможно, хотя бы потому, что невозможно полностью установить перечень угроз и способов их реализации. Поэтому надо выбрать из всего множества возможных воздействий лишь те, которые могут реально произойти и нанести серьезный ущерб владельцам и пользователям системы.

На этапе планирования формируется система защиты как единая совокупность мер противодействия различной природы.

По способам осуществления все меры обеспечения безопасности компьютерных систем подразделяются на: правовые, морально-этические, административные, физические и технические (аппаратные и программные) [9, с.28].

К правовым мерам защиты относятся действующие законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией ограниченного использования и ответственность за их нарушения. Этим они препятствуют несанкционированному использованию информации и являются сдерживающим фактором для потенциальных нарушителей.

К морально-этическим мерам противодействия относятся всевозможные нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают, как неписанные (например, общепризнанные нормы честности, патриотизма и т.п.), так и оформленные в некий свод (устав) правил или предписаний. Наиболее характерным примером последних является «Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США» [14]. В частности, считаются неэтичными умышленные или неумышленные действия, которые:

- нарушают нормальную работу компьютерных систем;

- вызывают дополнительные неоправданные затраты ресурсов (машинного времени, памяти, каналов связи и т.п.);

- нарушают целостность хранимой и обрабатываемой информации;

- нарушают интересы других законных пользователей и т.д.

**Административные меры защиты** — это меры организационного характера, регламентирующие процессы функционирования системы обработки информации, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности. Они включают:

- разработку правил обработки информации в АСОИБ;

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов АСОИБ (учет влияния стихии, пожаров, охрана помещений, организация защиты от установки прослушивающей аппаратуры и т.п.);

- мероприятия, осуществляемые при подборе и подготовке персонала (проверка новых сотрудников, ознакомление их с порядком работы с конфиденциальной информацией, с мерами ответственности за нарушение правил ее обработки; создание условий, при которых персоналу было бы невыгодно допускать злоупотребления и т.д.);

- организацию надежного пропускного режима;

- организацию учета, хранения, использования и уничтожения документов и носителей с конфиденциальной информацией;

- распределение реквизитов разграничения доступа (паролей, профилей полномочий и т.п.);

- организацию скрытого контроля за работой пользователей и персонала АСОИБ;

- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения (сертификация используемых технических и программных средств, строгое санкционирование, рассмотрение и утверждение всех изменений, проверка их на удовлетворение требованиям защиты, документальное отражение изменений и т.п.).

**Физические меры защиты** — это разного рода механические, электро- или электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации.

Техническими (аппаратно-программными) средствами защиты называются различные электронные устройства и специальные программы, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическую защиту информации и т.д.).

Наилучшие результаты достигаются при системном подходе к вопросам обеспечения безопасности АСОИБ и комплексном использовании различных мер защиты на всех этапах жизненного цикла системы, начиная с самых ранних стадий ее проектирования.

Очевидно, что в структурах с низким уровнем правопорядка, дисциплины и этики ставить вопрос о защите информации просто бессмысленно. Прежде всего надо решить правовые и организационные вопросы.

Административные меры играют значительную роль в обеспечении безопасности АСОИБ. Эти меры необходимо использовать тогда, когда другие методы и средства защиты просто недоступны (отсутствуют или слишком дороги). Однако это вовсе не означает, что систему защиты необходимо строить исключительно на основе административных методов, как это часто пытаются сделать чиновники, далекие от технического прогресса. Этим мерам присущи серьезные недостатки, такие как:

- низкая их надежность без соответствующей поддержки со стороны физических, технических и программных средств (люди склонны к нарушению любых установленных правил, если только их можно нарушить);

- применение для защиты только административного мер обычно приводит к параличу деятельности АСОИБ и всей организации (совершенно невозможно работать не нарушая инструкций) из-за ряда дополнительных неудобств, связанных с большим объемом рутинной формальной деятельности.

Административные меры надо везде, где только возможно, заменять более надежными современными физическими и техническими средствами. Они должны обеспечивать эффективное применение других, более надежных методов и средств защиты в части касающейся регламентации действий людей.

Известно не так много общих (универсальных) способов защиты АСОИБ от различных воздействий на нее. Ими являются:

- идентификация и аутентификация субъектов (пользователей, процессов и т.д.) АСОИБ;

- контроль доступа к ресурсам АСОИБ;

- регистрация и анализ событий, происходящих в АСОИБ;

- контроль целостности объектов АСОИБ;

- шифрование данных;

- резервирование ресурсов и компонентов АСОИБ.

Эти универсальные способы защиты могут применяться в различных вариациях и совокупностях в конкретных методах и средствах защиты.

Результатом этапа планирования является план защиты — документ, содержащий перечень защищаемых компонентов АСОИБ и возможных воздействий на них, цель защиты информации в АСОИБ, правила обработки информации в АСОИБ, обеспечивающие ее защиту от различных воздействий, а также описание разработанной системы защиты информации.

При необходимости, кроме плана защиты на этапе планирования может быть разработан план обеспечения непрерывной работы и восстановления функционирования АСОИБ, предусматривающий деятельность персонала и пользователей системы по восстановлению процесса обработки информации в случае различных стихийных бедствий и других критических ситуаций.

Сущность этапа реализации системы защиты заключается в установке и настройке средств защиты, необходимых для реализации зафиксированных в плане защиты правил обработки информации. Содержание этого этапа зависит от способа реализации механизмов защиты в средствах защиты.

К настоящему времени сформировались **два основных способа реализации механизмов защиты.**

**При первом** из них механизмы защиты не реализованы в программном и аппаратном обеспечении АСОИБ, либо реализована только часть их, необходимая для обеспечения работоспособности всей АСОИБ (например, механизмы защиты памяти в мультипользовательских системах). Защита информации при хранении, обработке или передаче обеспечивается дополнительными программными или аппаратными средствами, не входящими в состав самой АСОИБ. При этом средства защиты поддерживаются внутренними механизмами АСОИБ.

Такой способ получил название «добавленной» (add-on) защиты [6, с.87], поскольку средства защиты являются дополнением к основным программным и аппаратным средствам АСОИБ. Подобного подхода в обеспечении безопасности придерживается, например, фирма IBM, почти все модели ее компьютеров и ОС, от персональных до больших машин, используют добавленную защиту (например пакет RACF).

**Другой способ** носит название «встроенной» (built-in) защиты. Он заключается в том, что механизмы защиты являются неотъемлемой частью АСОИБ, разработанной и реализованной с учетом определенных требований безопасности. Механизмы защиты могут быть реализованы в виде отдельных компонентов АСОИБ, распределены по другим компонентам системы (то есть в некотором компоненте АСОИБ есть часть, отвечающая за поддержание его защиты). При этом средства защиты составляют единый механизм, который отвечает за обеспечение безопасности всей АСОИБ.

Этот способ использовался компанией DEC при разработке системы VAX/VMS.

Оба способа — добавленной и встроенной защиты — имеют свои преимущества и недостатки. Добавленная защита является более гибкой, ее механизмы можно добавлять или удалять по мере необходимости. Это не составит большого труда, так как они все реализованы отдельно от других процедур системы. Однако в этом случае остро встает вопрос поддержки работы этих механизмов встроенными механизмами ОС, в том числе и аппаратными. В том случае, если добавляемые средства защиты не поддерживаются встроенными механизмами АСОИБ, то они не обеспечат необходимого уровня безопасности.

Проблемой может стать сопряжение встроенных механизмов с добавляемыми программными средствами — довольно сложно разработать конфигурацию механизмов защиты, их интерфейс с добавляемыми программными средствами так, чтобы защита охватывала всю систему целиком.

Другой проблемой является оптимальность защиты. При любой проверке прав, назначении полномочий, разрешений доступа и т.д. необходимо вызывать отдельную процедуру. Естественно, это сказывается на производительности системы. Не менее важна и проблема совместимости защиты с имеющимися программными средствами. Как правило, при добавленной защите вносятся некоторые изменения в логику работы системы. Эти изменения могут оказаться неприемлемыми для некоторых прикладных программ. Такова плата за гибкость и облегчение обслуживания средств защиты.

**Основное достоинство встроенной защиты — надежность и оптимальность.** Это объясняется тем, что средства защиты и механизмы их поддержки разрабатывались и реализовывались одновременно с самой системой обработки информации, поэтому взаимосвязь средств защиты с различными компонентами системы теснее, чем при добавленной защите. Однако встроенная защита обладает жестко фиксированным набором функций, не позволяя расширять или сокращать их. Некоторые функции можно только отключить.

Справедливости ради стоит отметить, что оба вида защиты в чистом виде встречаются редко. Как правило, используются их комбинации, что позволяет объединять достоинства и компенсировать недостатки каждого из них.

Комплексная защита АСОИБ может быть реализована как с помощью добавленной, так и встроенной защиты.

Этап сопровождения заключается в контроле работы системы, регистрации происходящих в ней событий, их анализе с целью обнаружить нарушения безопасности.

В том случае, когда состав системы претерпел существенные изменения (смена вычислительной техники, переезд в другое здание, добавление новых устройств или программных средств), требуется повторение описанной выше последовательности действий.

Стоить отметить тот немаловажный факт, что обеспечение защиты АСОИБ — это **итеративный процесс**, завершающийся только с завершением жизненного цикла всей системы.

На последнем этапе анализа риска производится оценка реальных затрат и выигрыша от применения предполагаемых мер защиты. Величина выигрыша может иметь как положительное, так и отрицательное значение. В первом случае это означает, что использование системы защиты приносит очевидный выигрыш, а во втором - лишь дополнительные расходы на обеспечение собственной безопасности.

Сущность этого этапа заключается в анализе различных вариантов построения системы защиты и выборе оптимального из них по некоторому критерию (обычно по наилучшему соотношению «эффективность/стоимость»).

Приведем пример: необходимо оценить выгоду при защите информации от раскрытия или обработки на основе некорректных данных в течении одного года. [2, с.141]

Величину ущерба от реализации этих угроз оценим в $1.000.000. Предположим, предварительный анализ показал, что в среднем эта ситуация встречается один раз в десять лет (Р=0.1).

Тогда стоимость потерь для данной угрозы (СР) составит:

СР = С \* Р = $1.000.000 \* 0.1 = $100.000

Далее зададимся эффективностью методов защиты. Для данного абстрактного случая предположим, что в результате экспертной оценки методов защиты было получено значение 60% (в шести случаях из десяти защита срабатывает), тогда:

ЕМ = 60% \* СР = $60.000

Затраты на реализацию этих методов (закупка средств защиты, обучение персонала, изменение технологии обработки информации, зарплата персоналу и т.д.) составили (СМ) $25.000. Тогда величина выгоды равна:

PR = ЕМ - СМ = $60.000 - $25.000 = $35.000.

В рассмотренном случае величина выгоды имеет положительное значение, что говорит о целесообразности применения выбранных методов защиты.

После того, как были определены угрозы безопасности АСОИБ, от которых будет производится защита и выбраны меры защиты, требуется составить ряд документов, отражающих решение администрации АСОИБ по созданию системы защиты. Это решение конкретизируется в нескольких планах: плане защиты и плане обеспечения непрерывной работы и восстановления функционирования АСОИБ.

План защиты — это документ, определяющий реализацию системы защиты организации и необходимый в повседневной работе. Он необходим:

1. Для определения, общих правил обработки информации в АСОИБ, целей построения и функционирования системы защиты и подготовки сотрудников.

2. Для фиксирования на некоторый момент времени состава АСОИБ, технологии обработки информации, средств защиты информации.

3. Для определения должностных обязанностей сотрудников организации по защите информации и ответственности за их соблюдение.

План представляет собой организационный фундамент, на котором строится все здание системы защиты. Он нуждается в регулярном пересмотре и, если необходимо, изменении.

**План защиты** обычно содержит следующие группы сведений:

1. Политика безопасности.

2. Текущее состояние системы.

3. Рекомендации по реализации системы защиты.

4. Ответственность персонала.

5. Порядок ввода в действие средств защиты.

6. Порядок пересмотра плана и состава средств защиты.

Рассмотрим подробнее эти группы сведений.

**Политика безопасности.** В этом разделе должен быть определен набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение критичной информации в АСОИБ. Раздел должен содержать:

1. Цели, преследуемые реализацией системы защиты в вычислительной системе (например, защита данных компании от несанкционированного доступа, защита от утери данных и др.).

2. Меры ответственности средств защиты и нижний уровень гарантированной защиты (например, в работе небольших групп защищенных компьютеров, в обязанностях каждого из служащих и др.).

3. Обязательства и санкции, связанные с защитой (например, штрафы, персональная ответственность и др.).

**Рекомендации по реализации системы защиты**. Всесторонний анализ риска должен определять размеры наибольших возможных потерь, независимо от вероятности появления соответствующих событий; размеры наибольших ожидаемых потерь; меры, предпринимаемые в случае критических ситуаций, а также стоимость таких мер. Эти результаты используются при определении зон особого контроля и распределении средств для обеспечения защиты. В этом случае план защиты должен содержать рекомендации, какие средства контроля лучше всего использовать в чрезвычайных ситуациях (то есть имеющие наибольшую эффективность) и какие лучше всего соответствовали бы средствам контроля повседневной работы.

Некоторые ситуации могут приводить к слишком большому ущербу (например, крушение системы), а стоимость средств защиты от них может быть слишком высока или эти средства окажутся неэффективны. В этом случае лучше не учитывать такие ситуации при планировании защиты, хотя их и возникающие при этом возможные последствия следует отразить в плане.

**Ответственность персонала**. Каждый сотрудник обслуживающего персонала вычислительной системы должен хорошо знать свои обязанности и нести ответственность за свои действия. Ниже приводятся некоторые примеры обязанностей сотрудников и групп сотрудников:

1. Пользователь персонального компьютера или терминала несет ответственность за физическую целостность компьютера (терминала) во время сеанса работы с АСОИБ, а также за неразглашение собственного пароля.

2. Администратор баз данных несет ответственность за конфиденциальность информации в базах данных, ее логическую непротиворечивость и целостность.

3. Сотрудник руководства отвечает за разделение обязанностей служащих в сфере безопасности обработки информации, предупреждение возможных угроз и профилактику средств защиты.

**Порядок ввода в действие средств защиты**. Ввод в работу крупномасштабных и дорогих средств защиты целесообразно проводить постепенно, давая возможность обслуживающему персоналу и пользователям спокойно ознакомиться со своими новыми обязанностями. Для этого необходимо проводить разного рода тренировки, занятия по разъяснению целей защиты и способов ее реализации.

Этот раздел плана содержит расписание такого рода занятий, а также порядок ввода в действие системы защиты.

**Порядок модернизации средств защиты**. Важной частью плана защиты является порядок пересмотра состава средств защиты. Состав пользователей, данные, обстановка — все изменяется с течением времени, появляются новые программные и аппаратные средства. Многие средства защиты постепенно теряют свою эффективность и становятся ненужными, или подлежат замене по какой-либо иной причине (например, уменьшается ценность информации, для обработки которой достаточно более простых средств защиты). Поэтому список объектов, содержащих ценную информацию, их содержимое и список пользователей должны периодически просматриваться и изменяться в соответствии с текущей ситуацией. Также периодически должен проводиться анализ риска, учитывающий изменения обстановки. Последний пункт плана защиты должен устанавливать сроки и условия такого пересмотра, а также условия, при которых может производиться внеочередной пересмотр (например, качественный скачок в разработке методов преодоления защиты, что может нанести серьезный ущерб пользователям и владельцам АСОИБ).

Каким бы всеобъемлющим не был план, все возможные угрозы и защиту от них он предусмотреть не в состоянии. К тому же многие ситуации он должен только описывать — их контроль может оказаться неэффективным (в силу дороговизны средств защиты или малой вероятности появления угроз). В любом случае владельцы и персонал системы должны быть готовы к различным непредвиденным ситуациям.

Для определения действий персонала системы в критических ситуациях с целью обеспечения непрерывной работы и восстановления функционирования АСОИБ необходимо разрабатывать план **обеспечения непрерывной работы и восстановления** (план ОНРВ). В некоторых случаях план обеспечения непрерывной работы и план восстановления — разные документы. Первый скорее план, позволяющий избежать опасных ситуаций, второй — план реакции на них.

План ОНРВ можно сравнить с планом противопожарной защиты (обеспечение непрерывной работы) и ликвидации последствий (минимизация ущерба и восстановление функционирования АСОИБ). Про этот план обычно все знают, но никто его не читает, хотя на пепелище об этом обычно сожалеют.

Существует несколько способов смягчения воздействия непредвиденных ситуаций:

**1. Избегать их.** Это наиболее эффективный, но не всегда осуществимый способ. Избегать непредвиденных ситуаций можно с помощью ограничительных мер, предусмотренных планом защиты, а можно и с помощью устранения самой причины потенциального нарушения. Например, с пожаром можно бороться огнетушителем, а можно соблюдением мер противопожарной защиты. С рассерженными пользователями можно бороться административными мерами (разозлив этим их еще больше), а можно и поддержанием здоровой атмосферы в коллективе.

2. Если избежать какого-либо нарушения невозможно, необходимо **уменьшить вероятность** его появления или смягчить последствия от него.

3. Если предполагать, что какие-то нарушения все-таки могут произойти, следует предусмотреть меры **сохранения контроля над ситуацией**. Например, в любой момент может выйти из строя отдельный блок системы — часть компьютера, компьютер целиком, подсеть и т.д., может наступить нарушение энергоснабжения и др. В принципе это может привести к выходу АСОИБ из строя, однако при правильной организации АСОИБ этого можно избежать.

4. Если нарушение произошло, необходимо предусмотреть меры по **ликвидации последствий и восстановлению информации**. Например, в случае сбоя в компьютере — замену сбойного компонента, в случае уничтожения каких-либо данных — восстановление с резервных копий и т.д.

Все приведенные выше четыре способа должны в той или иной мере присутствовать в плане ОНРВ. Для каждой конкретной АСОИБ эти меры следует планировать в процессе анализа риска с учетом особенностей (специфических видов угроз, вероятностей появления, величин ущерба и т.д.) и на основе критерия «эффективность/стоимость». Хороший план ОНРВ должен отвечать следующим требованиям:

1. Реальность плана ОНРВ.

План должен оказывать реальную помощь в критических ситуациях, а не оставаться пустой формальностью. Необходимо учитывать психологический момент ситуации, при которой персонал находится в состоянии стресса, поэтому сам план и предлагаемые действия должны быть простыми и ясными. План должен учитывать реальное состояние компонентов системы, способов их взаимодействия и т.д. Повышению действенности плана ОНРВ способствуют тренировки в условиях, приближенных к реальным (естественно без реальных потерь).

2.Быстрое восстановление работоспособности системы.

Предлагаемые планом ОНРВ действия должны восстанавливать повседневную деятельность настолько быстро, насколько это возможно. В принципе это главное назначение плана ОНРВ. Расследовать причины и наказать виновных можно потом, главное — продолжить процесс обработки информации.

3. Совместимость с повседневной деятельностью.

Предлагаемые планом ОНРВ действия не должны нарушать привычный режим работы. Если его действия противоречат повседневной деятельности (возможно, возобновленной после аварии), то это приведет к еще большим проблемам.

4. Практическая проверка.

Все положения плана ОНРВ должны быть тщательно проверены, как теоретически, так и практически. Только в этом случае план ОНРВ будет удовлетворять перечисленным выше требованиям.

5. Обеспечение.

Реальная выполнимость плана ОНРВ будет достигнута только в том случае, если предварительно подготовлено, проверено и готово к работе все вспомогательное обеспечение — резервные копии, рабочие места, источники бесперебойного питания и т.д. Персонал должен совершенно точно знать, как и когда пользоваться этим обеспечением.

Наличие любого плана ОНРВ — полного или краткого, но главное —реального, благотворно влияет на моральную обстановку в коллективе. Пользователи должны быть уверены в том, что даже в самых неблагоприятных условиях какая-то часть их труда будет сохранена; руководство должно быть уверено, что не придется начинать все с начала.

План ОНРВ лучше всего строить как описание опасных ситуаций и способов реакции на них в следующем порядке:

- описание нарушения;

- немедленная реакция на нарушение - действия пользователей и администрации в момент обнаружения нарушения (сведение ущерба до минимума, уведомление руководства, останов работы, восстановительные процедуры и т.д.);

- оценка ущерба от нарушения — в чем заключаются потери и какова их стоимость (включая восстановление);

- возобновление обработки информации. После устранения нарушения и первичного восстановления необходимо как можно быстрее возобновить работу, так как машинное время — это деньги;

- полное восстановление функционирования системы - удаление и замена поврежденных компонентов системы, возобновление обработки информации в полном объеме.

В части, посвященной реакции на нарушения, план ОНРВ должен содержать перечень действий, которые выполняются персоналом при наступлении различных ситуаций. Причем действия должны быть реальными, иначе в них нет никакого смысла.

Эта часть плана должна определять:

- что должно быть сделано;

- когда это должно быть сделано;

- кем и как это должно быть сделано;

- что необходимо для того, чтобы это было сделано.

При планировании подобных действий необходимо помнить об их экономической эффективности. Например, всю информацию системы в резервных копиях держать в принципе невозможно — ее слишком много и она слишком часто обновляется. В копиях должна содержаться только самая ценная информация, значимость которой уменьшается не слишком быстро. Вообще определение степени дублирования ресурсов (критичной нагрузки; critical workload) — самостоятельная и достаточно сложная задача. Она должна решаться индивидуально для конкретных условий с учетом стоимости дублирования и загрузки системы, размеров возможного ущерба, имеющихся ресурсов и других факторов.

Для определения конкретных действий по восстановлению и возобновлению процесса обработки, включаемых в план ОНРВ, может быть полезен приводимый ниже список способов организации восстановления программ и данных, а также процесса обработки информации (первый способ для восстановления программ и данных, остальные — для возобновления самого процесса обработки информации).

Способы организации восстановления работы:

Резервное копирование и внешнее хранение программ и данных. Это основной и наиболее действенный способ сохранения программного обеспечения и данных. Резервные копии делаются с наборов данных, потеря или модификация которых могут нанести значительный ущерб. Обычно в таких копиях хранятся системное программное обеспечение и наборы данных, наиболее важное прикладное программное обеспечение, а также наборы данных, являющиеся основными в данной системе (например, база данных счетов в банке).

Резервное копирование может быть полным (копии делаются со всех наборов данных), возобновляемым (копии некоторых наборов данных периодически обновляются) и выборочным (копии делаются только с некоторых наборов данных, но потом не обновляются). Способы резервного копирования определяются для каждой конкретной АСОИБ индивидуально с точки зрения критерия экономической эффективности.

Резервное копирование не имеет никакого, смысла, если копии могут быть уничтожены вместе с оригиналами. Поэтому копии должны храниться в надежном месте, исключающем возможность уничтожения. В тоже время, должны существовать возможность их оперативного использования. Иногда хранят две и более копий каждого набора данных. Например, одна копия может храниться в сейфе, находящемся в границах доступа персонала системы, а другая — в другом здании. В случае сбоя оборудования в системе используется первая копия (оперативно!), а в случае ее уничтожения (например, при пожаре) — вторая.

Взаимодействие служб. Услуги по возобновлению процесса обработки предоставляются по взаимной договоренности другими службами или организациями, обычно безвозмездно. Взаимопомощь бывает двух видов:

1. Внешняя — другая организация предоставляет свою АСОИБ, возможно программное обеспечение для временной обработки информации пострадавшей стороной. Такой способ возобновления процесса обработки информации может использоваться для обработки небольших объемов некритичной информации. При этом желательно, чтобы две организации были примерно одного типа и работали в одной области.

2. Внутренняя — возможность обработки информации предоставляется другими подразделениями одной и той же организации (департаментами, отделами, группами). Такой способ обычно не требует больших затрат и легко доступен, если дублирующая АСОИБ позволяет проводить такого рода обработку.

**Любой план хорош в том случае, если он выполним**. Для обеспечения выполнимости планов необходимо чтобы работу по их составлению выполняла группа квалифицированных специалистов, размеры которой зависят от характера организации и масштабов предполагаемых мер защиты. Оптимальная численность группы 5-7 человек. Можно привлечь дополнительных сотрудников для обработки и анализа выводов и рекомендаций основной группы, или, в случае больших объемов работы, каждая группа должна составлять один план или один из пунктов плана.

Специализация сотрудников, входящих в группу разработки планов, зависит от конкретных условий. Использование защищенных протоколов, механизмов защиты операционных систем и сетей требует привлечения системных программистов. Применение средств защиты, встраиваемых в прикладное программное обеспечение делает необходимым участие в группе проблемных программистов. Необходимость организации защиты физических устройств, организации резервных рабочих мест также требует присутствия в рабочей группе соответствующих специалистов. И, наконец, поскольку АСОИБ функционирует для пользователя, то целесообразно присутствие пользователей различных категорий - для учета взгляда со стороны на удобство и эффективность предлагаемых методов и средств защиты. В большинстве случаев целесообразно, чтобы в эту группу входили следующие специалисты, каждый из которых должен отвечать за свой участок работы:

- специалисты по техническим средствам;

- системные программисты;

- проблемные программисты;

- сотрудники, отвечающие за подготовку, ввод и обработку данных;

- специалисты по защите физических устройств;

- представители пользователей.

После подготовки плана необходимо его принять и реализовать, что напрямую зависит от его четкости, корректности и ясности для сотрудников организации.

Понимание необходимости мер защиты и контроля - непременное условие нормальной работы. Известен случай о том, как пользователь менял каждый раз 24 пароля и возвращался к первоначальному, так как система была защищена от повторного использования предыдущих 23 паролей. Если сотрудники не понимают или не согласны с предлагаемыми мерами, то они будут стараться обойти их, так как любые меры контроля предполагают увеличение сложности работы.

Другой ключевой момент — управление средствами защиты и восстановления. Надежное управление осуществимо лишь в случае понимания обслуживающим персоналом размеров возможных убытков, ясного изложения планов и выполнения персоналом своих обязанностей. Многие сотрудники, обслуживающие АСОИБ, не всегда осознают риск, связанный с обработкой информации в АСОИБ. Только специальная предварительная подготовка персонала способствует правильной и эффективной работе средств защиты и восстановления; она может проводиться с привлечением сторонних специалистов. Описание различных способов преодоления и нарушения защиты в повседневной деятельности в сфере бизнеса (как, например, утечка информации к конкуренту) поможет обслуживающему персоналу понять необходимость точного выполнения требований защиты (например, своевременной смены паролей).

**Важнейшим понятием, которое должно быть оформлено документально, является политика безопасности.**

Политика безопасности — набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение критичной информации в системе. Она должна охватывать все особенности процесса обработки информации, определяя поведение системы в различных ситуациях.

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 АСОИБ 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 т.д.

Перед тем, как приступит к изложению материала введем некоторые определения.

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 этого способа, как правило, определяет название политики безопасности.

Для изучения свойств способа управления доступом создается его формальное описание — математическая модель. При этом модель должна отражать состояния всей системы, ее переходы из одного состояния в другое, а также учитывать, какие состояния и переходы можно считать безопасными в смысле данного управления. Без этого говорить о каких-либо свойствах системы, и тем более гарантировать их, по меньшей мере некорректно. Отметим лишь, что для разработки моделей применяется широкий спектр математических методов (моделирования, теории информации, графов, автоматов и другие).

В настоящее время лучше всего изучены **два вида политики безопасности:** избирательная и полномочная, основанные, соответственно на избирательном и полномочном способах управления доступом.

Кроме того, существует набор требований, усиливающий действие этих политик и предназначенный для управления информационными потоками в системе.

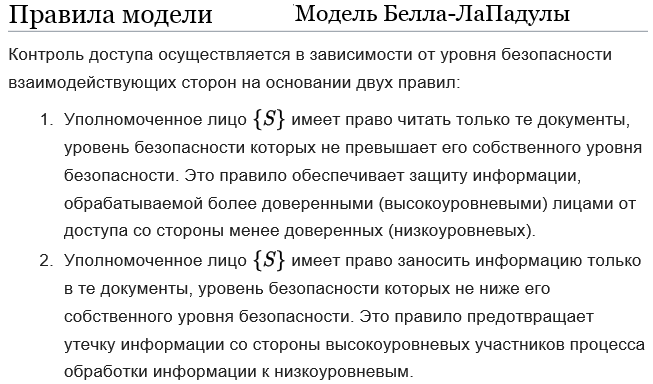
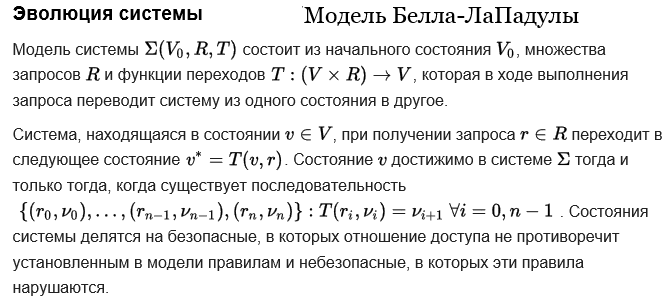
Следует отметить, что средства защиты, предназначенные для реализации какого-либо из названных выше способа управления доступом, только предоставляют возможности надежного управления доступом или информационными потоками. Определение прав доступа субъектов к объектам и/или информационным потокам (полномочий субъектов и атрибутов объектов, присвоение меток критичности и т д.) входит в компетенцию администрации системы.

Для того, чтобы корректно воплотить в жизнь разработанную политику безопасности необходимо иметь надежные механизмы ее реализации. Естественно предположить, что все средства, отвечающие 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.

Поэтому 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 АСОИБ. 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, то есть самой себя. ДВБ совместно используется всеми пользователями АСОИБ, однако ее модификация разрешена только пользователям со специальными полномочиями. К ним относятся администраторы системы и другие привилегированные сотрудники организации.

Процесс, функционирующий от имени ДВБ, является достоверным. 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. Сущность концепции заключается в том, что реальная система представляется как совокупность иерархически упорядоченных абстрактных уровней; при этом функции каждого уровня реализуются компонентами более низкого уровня. Компоненты определенного уровня зависят только от компонентов более низких уровней и их внутренняя структура полагается недоступной с более высоких уровней. Связь уровней организуется через межуровневый интерфейс.

Структура компонентов системы и связи между ними являются жестко фиксированными; их изменение, дублирование, уничтожение невозможны. Компоненты более высоких уровней привязаны к компонентам более низких уровней, те, в свою очередь, к элементам физической реализации (устройствам ввода-вывода, процессору и др.). Связи между различными компонентами определяются спецификациями межуровневого интерфейса и также не могут изменяться. Это является дополнительной мерой обеспечения целостности ДВБ.

Компоненты верхних уровней обычно описывают интерфейс пользователя. Сюда входят различные редакторы, компиляторы, интерпретаторы командных языков, утилиты и т.д. Средние уровни обычно реализуют ввод-вывод на уровне записей, работу с файлами и виртуальной памятью. Компоненты нижних уровней реализуют планирование и диспетчеризацию процессов, распределение ресурсов, ввод-вывод на физическом уровне, обработку прерываний и т.д. Компонентами нулевого уровня можно считать элементы физической реализации: особенности архитектуры процессора, состав и назначение регистров (общих и привилегированных), физическую реализацию некоторых функций и т.д. Множество компонентов всех уровней, кроме верхнего, а также средства управления ими и составляют ДВБ.

Пользователь, находясь на самом высоком уровне, может только послать запрос на выполнение какой-либо операции. Этот запрос будет разрешен к выполнению компонентами более низких уровней только в том случае, если, пройдя обработку корректности на всех промежуточных уровнях, он не был отвергнут, то есть не сможет нарушить существующую политику безопасности. При этом каждая функция может быть выполнена только определенными компонентами на определенном уровне, что определяется архитектурой системы в целом.

Например, пользователь из командного интерпретатора послал запрос на выполнение операции ввода-вывода (для редактирования файла, размещающегося на диске). Этот запрос будет обработан интерпретатором и передан на более низкий уровень — в подсистему ввода-вывода. Та проверит корректность запроса (разрешен ли доступ к этому файлу?), обработает его и передаст дальше — механизмам ввода-вывода, которые выполнят операцию и сообщат о результатах. При этом спецификации межуровневого интерфейса гарантируют, что прямой вызов примитивов ввода-вывода пользователю недоступен. Он еще может иногда обращаться непосредственно к подсистеме ввода-вывода (из программы), но не на более низкий уровень. Таким образом гарантируется невозможность доступа субъекта к объекту в обход средств контроля.

Необходимость защиты внутри отдельных компонентов системы очевидна: каждый из них должен проверять корректность обращения к реализуемой им функции.

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 самые механизмы, что и для защиты ДВБ. Теми же остаются и цели защиты: субъектов и объектов пользователей, в оперативной памяти и на внешних носителях. Рассмотрим подробнее принципы такой защиты.

Защита субъектов осуществляется с помощью межуровневого интерфейса: в зависимости от выполняемой им функции система переводит его на соответствующий уровень. Уровень, в свою очередь, определяет и степень управляемости процесса пользователем, который находится на самом верхнем уровне - чем ниже уровень процесса, тем меньше он управляем с более верхних уровней и тем больше он зависит от ОС.

Любые попытки защиты оперативной памяти приводят к необходимости создания виртуальной памяти в том или ином виде. Здесь используется та же концепция иерархической декомпозиции, чтобы отделить реальную память, содержащую информацию, от той, которая доступна пользователям. Соответствие между виртуальной и физической памятью обеспечивается диспетчером памяти. При этом различные области памяти могут являться компонентами разных уровней — это зависит от уровня программ, которые могут обращаться к этим областям.

Пользователи и их программы могут работать только с виртуальной памятью. Доступ к любому участку физической оперативной памяти (в том числе и принадлежащему ДВБ), контролируется диспетчером памяти. При трансляции виртуального адреса в физический проверяются права доступа к указанному участку. Надежность разделения оперативной памяти во многом обеспечивается за счет надежности функции, отображающей виртуальные адреса в физические: адресные пространства различных пользователей и системы не должны перекрываться в физической памяти.

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. Принятие решение на осуществление доступа осуществляется на основе информации, хранящейся в базе данных защиты. Сама база данных является частью ДВБ, доступ к ней также контролируется.

ДВБ должна быть организована таким образом, чтобы только ее компоненты могли выполнить запрос, причем только тот, который содержит корректные параметры.

Одним из необходимых условий реализации ДВБ в средствах защиты является наличие мультирежимного процессора (то есть процессора, имеющего привилегированный и обычный режим 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** является реализацией 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 др. программно-аппаратные средства, а также системные наборы данных.

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 или ее представления, которая служит основой избирательной политики безопасности.

**Важным понятием является понятие профиля.** Профилем называется список защищаемых объектов системы и прав доступа к ним, ассоциированный с каждым субъектом. При обращении к объекту профиль субъекта проверяется на наличие соответствующих прав доступа.

В системах с большим количеством объектов профили могут иметь большие размеры и, вследствие этого, ими трудно управлять; изменение профилей нескольких субъектов может потребовать большого количества операции и привести к трудностям в работе системы. Поэтому профили обычно используются лишь администраторами безопасности для контроля работы субъектов, и даже такое их применение весьма ограничено.

При реализации полномочной политики безопасности база данных защиты также содержит метки критичности всех объектов и уровни прозрачности субъектов системы.

**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 обладать следующими свойствами:

- 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.

В терминах модели Белла-Лападулла (избирательной и полномочной политик безопасности) монитор ссылок должен контролировать состояния системы и переходы из одного в другое. Основными функциями, которые должно выполнять **ядро безопасности** совместно с другими службами ОС, являются [2, с.193]:

1. Идентификация, аутентификация и авторизация субъектов и объектов системы.

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.

Эти функции необходимы для поддержания разрешительного порядка доступа к системе и соблюдения политики безопасности: авторизованный (разрешенный) доступ имеет только тот субъект, чей идентификатор удовлетворяет результатам аутентификации. Они выполняются как в процессе работы (при обращении к наборам данных, устройствам, ресурсам), так и при входе в систему.

2. Контроль входа пользователя в систему и управление паролями. Эти функции являются частным случаем перечисленных выше: 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). Однако при входе в систему существуют отличия при выполнении этих функций. Они обусловлены тем, что в процессе работы система уже имеет информацию о том, кто работает, какие у него полномочия (на основе информации в базе данных защиты) и т.д. и поэтому может адекватно реагировать на запросы субъекта. При входе в систему это все только предстоит определить. В данном случае возникает необходимость организации «достоверного маршрута» — пути передачи идентифицирующей информации от пользователя к ядру безопасности для подтверждения подлинности. Как показывает практика, вход пользователя в систему - одно из наиболее уязвимых мест защиты; известно множество случаев взлома пароля, входа без пароля, перехвата пароля 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, чья работа обеспечивается механизмами ДВБ, а также некоторыми другими механизмами, выполняющими вспомогательные функции. Они проверяют, например, что терминал, с которого осуществляется вход в систему, не занят никаким другим пользователем, который имитировал окончание работы.

3. Регистрация и протоколирование. Аудит.

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 безопасности системы. 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. Системный журнал является составной частью монитора ссылок и служит для контроля соблюдения политики безопасности. Он является одним из основных средств контроля, помогающим администратору предотвращать возможные нарушения в связи с тем, что:

- способен оперативно фиксировать происходящие в системе события;

- может помочь выявить средства и априорную информацию, использованные злоумышленником для нарушения;

- может помочь определить, как далеко зашло нарушение, подсказать метод его расследования и способы исправления ситуации.

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

4. Противодействие «сборке мусора».

После окончания 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». 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.

5. Контроль целостности субъектов.

Согласно модели Белла-Лападулла [2, с.196] множество субъектов системы есть подмножество множества объектов, то есть каждый субъект одновременно является объектом. При этом под содержимым субъекта обычно понимают содержимое контекста процесса, куда входит содержимое общих и специальных регистров (контекст процесса постоянно изменяется). Кроме содержимого или значения субъект имеет ряд специфических атрибутов: приоритет, список привилегий, набор идентификаторов и др. характеристики. В этом смысле поддержание целостности субъекта, то есть предотвращение его несанкционированной модификации, можно рассматривать как частный случай этой задачи для объектов вообще.

В то же время субъект отличается от объекта тем, что является, согласно определению, активным компонентом системы. В связи с этим для защиты целостности субъекта, в качестве представителя которого выступает процесс, вводится такое понятие как **рабочая среда** или область исполнения процесса. Эта область является логически защищенной подсистемой, которой доступны все ресурсы системы, относящиеся к соответствующему процессу. Другими словами, область исполнения процесса является виртуальной машиной. В рамках этой области процесс может выполнять любые санкционированные действия без опасения нарушения целостности. Таким образом, реализуется концепция защищенной области для отдельного процесса.

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: это действие называется переключением области процесса. Оно всегда связано с переходом центрального процессора в привилегированный режим работы.

Механизмы поддержки областей исполнения процесса обеспечивают контроль их целостности достаточно надежно. Однако даже разделенные процессы должны иметь возможность обмениваться информацией. Для этого разработаны несколько специальных механизмов, чтобы можно было осуществлять обмен информацией между процессами без ущерба безопасности или целостности каждого из них. К таким механизмам относятся, например, кластеры флагов событий, почтовые ящики и другие системные структуры данных. Следует однако учитывать, что с их помощью может осуществляться утечка информации, поэтому если использование таких механизмов разрешено, их обязательно следует контролировать.

6. 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 субъектом некоторой операции над объектом из множества разрешенных для данного типа. Примерами таких операций являются чтение, открытие, запись набора данных, обращение к устройству и т.д.

Контроль должен осуществляться при доступе к:

- оперативной памяти;

- разделяемым устройствам прямого доступа;

- разделяемым устройствам последовательного доступа;

- разделяемым программам и подпрограммам;

- разделяемым 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 случиться, все они попадают в круг подозреваемых.

Существует **четыре основных способа разделения субъектов** к совместно используемым объектам:

1. Физическое - субъекты обращаются к физически различным объектам (однотипным устройствам, наборам данных на разных носителях и т.д.).

2. Временное - субъекты с различными правами доступа к объекту получают его в различные промежутки времени.

3. 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»; в этом случае разделение может быть реализовано различными способами разделение оригинала объекта, разделение с копированием объекта и т.д.

4. Криптографическое - все объекты хранятся в зашифрованном виде, права доступа определяются наличием ключа для расшифрования объекта.

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

Контроль доступа субъектов системы к объектам (не только к совместно используемым, но и к индивидуальным) реализуется с помощью тех же механизмов, которые реализуют ДВБ и осуществляется процедурами ядра безопасности.

Как уже отмечалось выше, настройка механизмов защиты — дело сугубо индивидуальное для каждой системы и даже для каждой задачи. Поэтому дать ее подробное описание довольно трудно. Однако существуют общие принципы, которых следует придерживаться, чтобы облегчить себе работу, так как они проверены практикой. Рассмотрим их:

1.Группирование.

Это объединение множества субъектов под одним групповым именем; всем субъектам, принадлежащим одной группе, предоставляются равные права. Принципы объединения пользователей в группы могут быть самые разные: одинаковый характер вычислений, работа над совместным проектом и т.д. При этом один и тот же субъект может входить в несколько различных 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 групп очень важен, поскольку члены одной группы имеют доступ к большому числу объектов, что не способствует их безопасности. Создание групп и присвоение групповых привилегий должно производиться администратором безопасности, руководителем группы или каким-либо другим лицом, несущим ответственность за сохранность групповых объектов.

2. Правила умолчания.

Большое внимание при назначении привилегий следует уделять 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 кому-либо. 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.

3. Минимум привилегий.

Это один из основополагающих принципов реализации любой политики безопасности, используемый повсеместно. Каждый пользователь и процесс должен иметь минимальное число привилегий, необходимых 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.

4. Принцип «надо знать».

Этот принцип во многом схож с предыдущим. Согласно ему, полномочия пользователей назначаются согласно их обязанностям. Доступ разрешен только к той информации, которая необходима им для работы. Согласно принципу, пользователь должен знать обо всех доступных ему ресурсах. В том случае, если пользователь не знает о них, такие ресурсы должны быть отключены.

5. Объединение критичной информации.

Во многих системах сбор, хранение и обработка информации одного уровня производится в одном месте (узле сети, устройстве, каталоге). Это связано с тем, что проще защитить одним и тем же способом большой массив информации, чем организовать индивидуальную защиту для каждого набора данных. Для реализации этого принципа могут быть разработаны специальные программы, управляющие обработкой таких наборов данных. Это будет простейший способ построения защищенных областей.

6. 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.

Узлами нижележащих уровней являются администраторы подсистем, имеющие права изменять привилегии пользователей этих подсистем (в их роли могут выступать руководители организаций, отделов). Листьями дерева являются все пользователи системы. Вообще говоря, субъект, стоящий в корне любого поддерева, имеет право изменять защиту любого субъекта, принадлежащего этому поддереву.

Достоинство такой структуры — точное копирование схемы организации, которую обслуживает АСОИБ. 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.

7. Привилегии владельца.

При таком контроле каждому объекту соответствует единственный субъект с исключительным правом контроля объекта — владелец. Как правило, это его создатель. Владелец обладает всеми разрешенными для этого типа данных правами на объект, может разрешать доступ любому другому субъекту, но не имеет права никому 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 приводить к сложностям в работе (например; при отсутствии владельца или просто нежелании его разрешить доступ). Поэтому такой принцип обычно используется при защите личных объектов пользователей.

8. Свободная передача привилегий.

При такой схеме субъект, создавший объект, может передать любые права на него любому другому субъекту. Тот, в свою очередь, может передать все эти права другому субъекту.

Естественно, при этом возникают большие трудности в определении круга субъектов, имеющих в данный момент доступ к объекту (права на объект могут распространяться очень быстро и так же быстро исчезать), и поэтому такой объект легко подвергнуть несанкционированной обработке. В силу этих обстоятельств подобная схема применяется достаточно редко — в основном в исследовательских группах, работающих над одним проектом (когда все имеющие доступ к объекту заинтересованы в его содержимом).

В чистом виде рассмотренные принципы реализации политики безопасности применяются редко. Обычно используются их различные комбинации. Ограничение доступа к объектам в ОС включает в себя ограничение доступа к некоторым системным возможностям, например, ряду команд, программам и т.д., если при использовании их нарушается .политика безопасности. Вообще набор полномочий каждого пользователя должен быть тщательно продуман, исключены возможные противоречия и дублирования, поскольку большое количество нарушений происходит именно из-за этого. Может произойти утечка информации без нарушения защиты, если плохо была спроектирована или реализована политика безопасности.

**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 реализовываться 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.

Имеется два подхода к обеспечению безопасности АСОИБ.

**«Фрагментарный» подход** ориентируется на противодействие строго определенным угрозам при определенных условиях. Примерами реализации такого подхода являются, например, специализированные антивирусные средства, отдельные средства регистрации и управления, автономные средства шифрования и т.д. Главная отличительная особенность «фрагментарного» подхода — отсутствие единой защищенной среды обработки информации.

Главным достоинством «фрагментарного» подхода является его высокая избирательность относительно конкретной угрозы, обуславливающая и основной его недостаток — локальность действия. Другими словами, фрагментарные меры защиты обеспечивают эффективную защиту конкретных объектов АСОИБ от конкретной угрозы, но не более того. Даже небольшое видоизменение угрозы ведет к потере эффективности защиты; распространить действие таких мер на всю АСОИБ практически невозможно.

Особенностью **комплексного подхода** является создание защищенной среды обработки информации в АСОИБ, объединяющей разнородные меры противодействия угрозам (правовые, организационные, программно-технические). Защищенная среда обработки информации строится на основе разработанных для конкретной АСОИБ правил обработки критической информации.

Организация защищенной среды обработки информации позволяет гарантировать (в рамках разработанной политики безопасности) уровень безопасности АСОИБ. Недостатками подхода являются высокая чувствительность к ошибкам установки и настройки средств защиты, сложность управления, ограничения на свободу действий пользователей АСОИБ.

Комплексный подход применяют для защиты крупных АСОИБ, или небольших АСОИБ, обрабатывающих дорогостоящую информацию или выполняющих ответственные задачи. При этом способ реализации комплексной защиты определяется спецификой АСОИБ, другими объективными и субъективными факторами.

Для всех крупных организаций характерно то, что нарушение безопасности информации в их АСОИБ может нанести огромный материальный ущерб как самим организациям, так и их клиентам. Поэтому эти организации вынуждены особое внимание уделять гарантиям безопасности, что ведет к необходимости реализации комплексной защиты.

Комплексного подхода придерживаются большинство государственных и крупных коммерческих предприятий и учреждений, он нашел свое отражение в различных стандартах и целенаправленно проводится в жизнь, например, Министерством обороны США в лице Национального Центра Компьютерной Безопасности (NCSC). [2, с.201]

Важным компонентом защиты является **«горячий резерв».**

«Горячий резерв» используется для возобновления процесса обработки после событий, вызвавших полный или частичный отказ основной системы — в результате отключения энергоснабжения, неисправности оборудовании или программного обеспечения, злого умысла («вирусная атака») и т.д.

«Горячий резерв» — это готовая к работе дублирующая система, в которой полностью сгенерирована операционная система, размещены прикладное программное обеспечение и наборы данных. Кроме того, резервная система должна иметь работоспособные периферийные устройства, подключенные каналы связи, источники энергоснабжения и даже персонал. Время на подготовку определяется временем загрузки резервных копий и системы.

Содержание «горячего резерва» обходится очень дорого. Однако в некоторых случаях — для обработки информации, требующей полного контроля со стороны ее владельца, «горячий резерв» необходим. Кроме того, можно содержать и использовать «горячий резерв» на кооперативных началах — вместе с другими организациями.

**«Расщепленный резерв»** представляет собой способ не столько восстановления, сколько организации АСОИБ. В этом смысле о нем можно говорить, как о способе организации системы с высокой степенью распределенности и взаимодублирующими составными частями. При таком подходе критичные элементы системы (аппаратура, программы, данные) разнесены по отдельным ее частям (узлам распределенной системы) и функционируют в какой-то мере независимо, обмениваясь между собой информацией по каналам связи.

В случае выхода из строя отдельных элементов системы другие могут взять на себя их функции. Времени на приведение дублирующих элементов в рабочее состояние очень мало, фактически оно определяется загрузкой из резервных копий (так как аппаратура расщепленного резерва всегда находится в рабочем состоянии).

Такой способ обеспечения непрерывной работы и восстановления очень эффективен, так как позволяет быстро осуществлять переход с основных элементов АСОИБ на дублирующие. Более того, этот переход может быть практически незаметен для пользователей за исключением возрастания нагрузки на отдельные элементы. Однако при использовании «расщепленного резерва» возникает множество проблем, основными из которых являются:

1. Определение критической нагрузки. Распределение аппаратуры, программ и данных по элементам всей АСОИБ таким, чтобы обеспечить оптимальное дублирование и восстановление данных и процесса их обработки в различных ситуациях. Существующие математические методы позволяют рассчитывать оптимальную критическую нагрузку для каждого конкретного случая.

2. Обеспечение безопасности. При распределении программ и данных по различным элементам системы неизбежно увеличивается вероятность различных нарушений. Эта вероятность повышается в критических случаях, когда информация может обрабатываться на других элементах системы, возможно, с нарушением безопасности. В этом случае необходимо разрабатывать политику безопасности и составлять планы с учетом возможных опасных ситуаций и реакции на них.

**«Холодный резерв»** используется для возобновления процесса обработки после серьезных, нанесший большой ущерб событий, которые привели к полному выходу системы из строя пожара, наводнения и т.д. Время на восстановление в этом случае может исчисляться неделями и месяцами. Естественно, это слишком большой срок, чтобы позволить себе обходиться без обработки информации.

«Холодный резерв» представляет собой резервную систему обработки данных, которая не участвует в повседневной деятельности организации. Резервная система поставляется определенными фирмами (по заранее согласованной договоренности) в течение короткого промежутка времени (24 часа). Так же оперативно выполняются пуско-наладочные работы, после чего резервная система готова принять на себя функции основной.

В результате подобных мероприятий перерыв в работе АСОИБ в результате полного и необратимого выхода ее из строя будет исчисляться днями, а не неделями и месяцами. В то же время, покупка и установка резервной системы — дело дорогое, к тому же она не сможет принять на себя все функции основной, а только некоторую их часть. Поэтому «холодный резерв» целесообразно использовать для возобновления выполнения наиболее важных операций.

В том случае, когда размер ущерба невелик, система серьезно не пострадала, то наилучшим способом может быть отсутствие экстренных действий и продолжение работы.

Важным понятием политики безопасности является **избирательная политика безопасности**

Основой избирательной политики безопасности является **избирательное управление доступом** (ИУД), 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 типов 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 передать 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 АСОИБ.

Вследствие больших размеров и разреженности МД хранение полной матрицы представляется нецелесообразным, поэтому во многих средствах защиты используют более экономные представления МД (профили). Каждый из этих способов представления МД имеет свои достоинства и 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.

Основу **полномочной политики безопасности** составляет полномочное управление доступом, которое подразумевает, что:

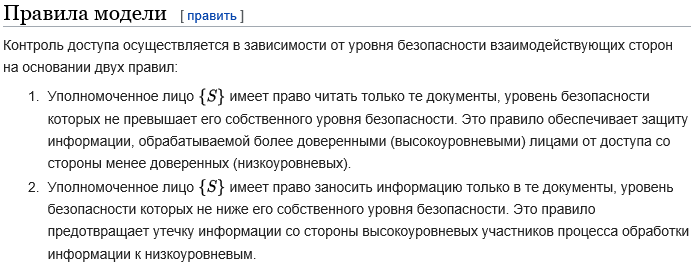
- все субъекты и объекты системы должны быть однозначно идентифицированы;

- каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;

- каждому субъекту системы присвоен уровень прозрачности, 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 ненисходящий (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 [2, с.159], включающая в себя понятия 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» и «свойством». 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.

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 проникновении с нижних уровней на верхние. При этом она функционирует на фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности).

Изначально полномочная политика безопасности была разработана в интересах минобороны США для обработки информации с различными грифами секретности. Ее применение в коммерческом секторе сдерживается следующими основными причинами :

- отсутствием в коммерческих организациях четкой классификации хранимой и 'обрабатываемой информации, аналогичной государственной классификации (грифы секретности сведений);

- высокой стоимостью реализации и большими накладными расходами.

Помимо управления доступом субъектов к объектам системы проблема защиты информации имеет еще один аспект. Чтобы получить информацию о каком-либо объекте системы, 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**. По этим каналам можно получать информацию не только о содержимом объекта, но и о его состоянии, атрибутах и др. в зависимости от особенностей системы и установленной защиты объектов. Эта особенность связана с тем, что при взаимодействии двух субъектов возникает некоторый поток информации от одного к другому.

Информационные потоки существуют в системе всегда. Поэтому возникает необходимость определить, какие информационные потоки в системе являются «легальными», то есть 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 называется **потоковой** [2, с.176]. 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. Управление информационными потоками применяется обычно в рамках избирательной или полномочной политики, дополняя их и повышая надежность системы защиты.

Управление доступом (избирательное или полномочное) сравнительно легко реализуемо (аппаратно или программно), однако оно неадекватно реальным АСОИБ 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 такого управления в полном объеме достаточна сложна, поэтому его обычно используют для усиления надежности **полномочной** политики: ненисходящие (относительно уровней безопасности) информационные потоки считаются разрешенными, все остальные — запрещенными.

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

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