Гайкович В.Ю., Ершов Д.В.

Основы безопасности информационных технологий

СОДЕРЖАНИЕ

Общеизвестно, что любое фундаментальное техническое или технологическое новшество, предоставляя возможности для решения одних социальных проблем и открывая широкие перспективы их развития, всегда вызывает обострение других или порождает новые, ранее неизвестные проблемы, становится для общества источником новых потенциальных опасностей. Если в должной мере не позаботиться о нейтрализации сопутствующих прогрессу негативных факторов, то эффект от внедрения новейших достижений науки и техники может оказаться в целом отрицательным. Иными словами, без должного внимания к вопросам обеспечения безопасности последствия перехода общества к новым технологиям могут быть катастрофическими для него и его граждан. Именно так обстоит дело в области атомных, химических и других экологически опасных технологий, в сфере транспорта. Аналогично обстоит дело и с информатизацией общества.

Бурное развитие средств вычислительной техники открыло перед человечеством небывалые возможности по автоматизации умственного труда и привело к созданию большого числа разного рода автоматизированных информационных и управляющих систем, к возникновению принципиально новых, так называемых, информационных технологий.

Неправомерное искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляющих системах наносят серьезный материальный и моральный урон многим субъектам (государству, юридическим и физическим лицам), участвующим в процессах автоматизированного информационного взаимодействия.

Жизненно важные интересы этих субъектов, как правило, заключаются в том, чтобы определенная часть информации, касающаяся их безопасности, экономических, политических и других сторон деятельности, конфиденциальная коммерческая и персональная информация, была бы постоянно легко доступна и в то же время надежно защищена от неправомерного ее использования: нежелательного разглашения, фальсификации, незаконного тиражирования или уничтожения.

Острота проблемы обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных и управляющих систем, хранящейся и обрабатываемой в них информации все более возрастает. Этому есть целый ряд объективных причин.

Прежде всего - это расширение сферы применения средств вычислительной техники и возросший уровень доверия к автоматизированным системам управления и обработки информации. Компьютерным системам дове-

ряют самую ответственную работу, от качества выполнения которой зависит жизнь и благосостояние многих людей. ЭВМ управляют технологическими процессами на предприятиях и атомных электростанциях, управляют движением самолетов и поездов, выполняют финансовые операции, обрабатывают секретную и конфиденциальную информацию.

Изменился подход и к самому понятию "информация". Этот термин все чаще используется для обозначения особого товара, стоимость которого зачастую превосходит стоимость вычислительной системы, в рамках которой он существует. Осуществляется переход к рыночным отношениям в области создания и предоставления информационных услуг, с присущей этим отношениям конкуренцией и промышленным шпионажем.

Проблема защиты вычислительных систем становится еще более серьезной и в связи с развитием и распространением вычислительных сетей, территориально распределенных систем и систем с удаленным доступом к совместно используемым ресурсам.

Доступность средств вычислительной техники и прежде всего персональных ЭВМ привела к распространению компьютерной грамотности в широких слоях населения, что закономерно, привело к увеличению числа попыток неправомерного вмешательства в работу государственных и коммерческих автоматизированных систем как со злым умыслом, так и чисто "из спортивного интереса". К сожалению, многие из этих попыток имеют успех и наносят значительный урон всем заинтересованным субъектам информационных отношений.

Положение усугубляется тем, что практически отсутствует законодательное (правовое) обеспечение защиты интересов субъектов информационных отношений. Отставание в области создания стройной и непротиворечивой системы законодательно-правового регулирования отношений в сфере накопления и использования информации создает условия для возникновения и распространения "компьютерного хулиганства" и "компьютерной преступности".

Еще одним весомым аргументом в пользу усиления внимания к вопросам безопасности вычислительных систем является бурное развитие и распространение так называемых компьютерных вирусов, способных скрытно существовать в системе и совершать потенциально любые несанкционированные действия.

Особую опасность для компьютерных систем представляют злоумышленники, специалисты - профессионалы в области вычислительной техники и программирования, досконально знающие все достоинства и слабые места вычислительных систем и располагающие подробнейшей документацией и самыми совершенными инструментальными и технологическими средствами для анализа и взлома механизмов защиты.

При выработке подходов к решению проблемы компьютерной, информационной безопасности следует всегда исходить из того, что защита информации и вычислительной системы не является самоцелью. Конечной целью создания системы компьютерной безопасности является защита всех категорий субъектов, прямо или косвенно участвующих в процессах информационного взаимодействия, от нанесения им ощутимого материального, морального или иного ущерба в результате случайных или преднамеренных воздействий на информацию и системы ее обработки и передачи.

В качестве возможных нежелательных воздействий на компьютерные системы должны рассматриваться: преднамеренные действия злоумышленников, ошибочные действия обслуживающего персонала и пользователей системы, проявления ошибок в ее программном обеспечении, сбои и отказы оборудования, аварии и стихийные бедствия.

В качестве защищаемых объектов должны рассматриваться информация и все ее носители (отдельные компоненты и автоматизированная система обработки информации в целом).

Обеспечение безопасности вычислительной системы предполагает создание препятствий для любого несанкционированного вмешательства в процесс ее функционирования, а также для попыток хищения, модификации, выведения из строя или разрушения ее компонентов, то есть защиту всех компонентов системы: оборудования, программного обеспечения, данных (информации) и ее персонала.

В этом смысле защита информации от несанкционированного доступа (НСД) является только частью общей проблемы обеспечения безопасности компьютерных систем и защиты законных интересов субъектов информационных отношений, а сам термин НСД было бы правильнее трактовать не как "несанкционированный доступ" (к информации), а шире, - как "несанкционированные (неправомерные) действия", наносящие ущерб субъектам информационных отношений.

Важность и сложность проблемы защиты информации в автоматизированных системах обработки информации (АС) требует принятия кардинальных мер, выработки рациональных решений, для чего необходимо сконцентрировать усилия на вопросах разработки общей концепции защиты интересов всех субъектов информационных отношений с учетом особенностей тех прикладных областей, в которых функционируют различные АС.

Исследования проблемы обеспечения безопасности компьютерных систем ведутся как в направлении раскрытия природы явления, заключающегося в нарушении целостности и конфиденциальности информации, дезорганизации работы компьютерной системы, так и в направлении разработки конкретных практических методов и средств их защиты. Серьезно изучается статистика нарушений, вызывающие их причины, личности нарушителей,

суть применяемых нарушителями приемов и средств, используемые при этом недостатки систем и средств их защиты, обстоятельства, при которых было выявлено нарушение, и другие вопросы.

Необходимость проведения настоящей работы вызвана отсутствием необходимых научно-технических и методических основ обеспечения защиты информации в современных условиях, в частности, в компьютерных банковских системах. Имеются веские основания полагать, что применяемые в настоящее время в отечественных системах обработки банковской информации организационные меры и особенно аппаратно-программные средства защиты не могут обеспечить достаточную степень безопасности субъектов, участвующих в процессе информационного взаимодействия, и не способны в необходимой степени противостоять разного рода воздействиям с целью доступа к финансовой информации и дезорганизации работы автоматизированных банковских систем.

Ориентируясь при рассмотрении вопросов информационной безопасности в основном на банковскую специфику, авторы тем не менее старались достичь максимального уровня общности приводимых определений, результатов анализа и выводов везде, где это было возможно.

1. ОСНОВНЫЕ ПОНЯТИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Цель данного раздела - дать определения основных понятий в области безопасности информационных технологий, сформулировать цели обеспечения безопасности.

Прежде всего необходимо разобраться, что такое безопасность информационных отношений, определить что (кого), от чего, почему и зачем надо защищать. Только получив четкие ответы на данные вопросы, можно правильно сформулировать общие требования к системе обеспечения безопасности и переходить к обсуждению вопросов построения соответствующей защиты.

Информация и информационные отношения. Субъекты информационных отношений, их безопасность

В данной работе под информацией будем понимать сведения о фактах, событиях, процессах и явлениях, о состоянии объектов (их свойствах, характеристиках) в некоторой предметной области, используемые (необходимые) для оптимизации принимаемых решений в процессе управления данными объектами.

Информация может существовать в различных формах в виде совокупностей некоторых знаков (символов, сигналов и т.п.) на носителях различных типов. В связи с бурным процессом информатизации общества все большие объемы информации накапливаются, хранятся и обрабатываются в автоматизированных системах, построенных на основе современных средств вычислительной техники и связи. В данной работе будут рассматриваться только те формы представления информации, которые используются при ее автоматизированной обработке.

В дальнейшем субъектами будем называть государство (в целом или отдельные его органы и организации), общественные или коммерческие организации (объединения) и предприятия (юридических лиц), отдельных граждан (физических лиц).

В процессе своей деятельности субъекты могут находиться друг с другом в разного рода отношениях, в том числе, касающихся вопросов получения, хранения, обработки, распространения и использования определенной информации. Такие отношения между субъектами будем называть *информационными отношениями*, а самих участвующих в них субъектов - *субъектами информационных отношений*.

Под автоматизированной системой обработки информации (АС) будем понимать организационно-техническую систему, представляющую собой совокупность следующих взаимосвязанных компонентов:

- технических средств обработки и передачи данных (средств вычислительной техники и связи);
- методов и алгоритмов обработки в виде соответствующего программного обеспечения;
- информации (массивов, наборов, баз данных) на различных носителях;
- персонала и пользователей системы, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки информации (данных) с целью удовлетворения информационных потребностей субъектов информационных отношений.

Под обработкой информации в АС будем понимать любую совокупность операций (прием, сбор, накопление, хранение, преобразование, отображение, выдача и т.п.), осуществляемых над информацией (сведениями, данными) с использованием средств АС.

Различные субъекты по отношению к определенной информации могут выступать в качестве (возможно одновременно):

- источников (поставщиков) информации;
- пользователей (потребителей) информации;
- собственников (владельцев, распорядителей) информации;
- физических и юридических лиц, о которых собирается информация;
- владельцев систем сбора и обработки информации и участников процессов обработки и передачи информации и т.д.

Для успешного осуществления своей деятельности по управлению объектами некоторой предметной области субъекты информационных отношений могут быть заинтересованы в обеспечении:

- своевременного доступа (за приемлемое для них время) к необходимой им информации;
- конфиденциальности (сохранения в тайне) определенной части информации;
- достоверности (полноты, точности, адекватности, целостности) информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);
- защиты части информации от незаконного ее тиражирования (защиты авторских прав, прав собственника информации и т.п.);

- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации.

Будучи заинтересованным в обеспечении хотя бы одного из вышеназванных требований субъект информационных отношений является уязвимым, то есть потенциально подверженным нанесению ему ущерба (прямого или косвенного, материального или морального) посредством воздействия на критичную для него информацию и ее носители либо посредством неправомерного использования такой информации. Поэтому все субъекты информационных отношений заинтересованы в обеспечении своей информационной безопасности (конечно в различной степени в зависимости от величины ущерба, который им может быть нанесен).

Для удовлетворения законных прав и перечисленных выше интересов субъектов (обеспечения их информационной безопасности) необходимо постоянно поддерживать следующие свойства информации и систем ее обработки:

- ***доступность информации***, то есть свойство системы (среды, средств и технологии ее обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость;
- ***целостность информации***, то есть свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). Точнее говоря, субъектов интересует обеспечение более широкого свойства - достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, то есть ее неискаженности. Однако, мы ограничимся только рассмотрением вопросов обеспечения целостности информации, так как вопросы обеспечения адекватности отображения выходят далеко за рамки проблемы обеспечения информационной безопасности;
- ***конфиденциальность информации*** - субъективно определяемую (приписываемую) характеристику (свойство) информации, указывающую на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемую способно-

стью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты законных интересов других субъектов информационных отношений.

Поскольку ущерб субъектам информационных отношений может быть нанесен опосредовано, через определенную информацию и ее носители (в том числе автоматизированные системы обработки), то закономерно возникает заинтересованность субъектов в обеспечении безопасности этой информации и систем ее обработки и передачи. Иными словами, в качестве объектов, подлежащих защите в интересах обеспечения безопасности субъектов информационных отношений, должны рассматриваться: информация, ее носители и процессы ее обработки.

Однако, всегда следует помнить, что уязвимыми в конечном счете являются именно заинтересованные в обеспечении определенных свойств информации и систем ее обработки субъекты (информация, равно как и средства ее обработки, не имеет своих интересов, которые можно было бы ущемить и нанести тем самым ущерб). В дальнейшем, говоря об обеспечении безопасности АС или циркулирующей в системе информации, всегда будем понимать под этим косвенное обеспечение безопасности субъектов, участвующих в процессах автоматизированного информационного взаимодействия.

В свете сказанного, термин "безопасность информации" нужно понимать как *защищенность* информации от нежелательного для соответствующих субъектов информационных отношений ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Поскольку субъектам информационных отношений ущерб может быть нанесен также посредством воздействия на процессы и средства обработки критичной для них информации, то становится очевидной необходимость обеспечения защиты всей системы обработки и передачи данной информации от несанкционированного вмешательства в процесс ее функционирования, а также от попыток хищения, незаконной модификации и/или разрушения любых компонентов данной системы.

Поэтому под безопасностью автоматизированной системы обработки информации (компьютерной системы) будем понимать защищенность всех ее компонентов (технических средств, программного обеспечения, данных и персонала) от подобного рода нежелательных для соответствующих субъектов информационных отношений воздействий.

Безопасность любого компонента (ресурса) АС складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности.

Конфиденциальность компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

Целостность компонента системы предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени.

Доступность компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

В свете приведенного выше подчеркнем, что конечной целью защиты АС и циркулирующей в ней информации является предотвращение или минимизация наносимого субъектам информационных отношений ущерба (прямого или косвенного, материального, морального или иного) посредством нежелательного воздействия на компоненты АС, а также разглашения (утечки), искажения (модификации), утраты (снижения степени доступности) или незаконного тиражирования информации.

Наибольшую сложность при решении вопросов обеспечения безопасности конкретных информационно-управляющих систем (информационных технологий) представляет задача определения реальных требований к уровням защиты критичной для субъектов информации, циркулирующей в АС. Ориентация на интересы субъектов информационных отношений дает ключ к решению данной задачи для общего случая.

Определение требований к защищенности информации

Исторически сложившийся подход к классификации государственной информации (данных) по уровням требований к ее защищенности основан на рассмотрении и обеспечении только одного свойства информации - ее конфиденциальности (секретности). Требования же к обеспечению целостности и доступности информации, как правило, лишь косвенно фигурируют среди общих требований к системам обработки этих данных. Считается, что раз к информации имеет доступ только узкий круг доверенных лиц, то вероятность ее искажения (несанкционированного уничтожения) незначительна. Низкий уровень доверия к АС и предпочтение к бумажной информационной технологии еще больше усугубляют ограниченность данного подхода.

Если такой подход в какой-то степени оправдан в силу существующей приоритетности свойств безопасности важной государственной информации,

то это вовсе не означает, что его механический перенос в другую предметную область (с другими субъектами и их интересами) будет иметь успех.

Во многих областях деятельности (предметных областях) доля конфиденциальной информации сравнительно мала. Для коммерческой и персональной информации, равно как и для государственной информации, не подлежащей засекречиванию, приоритетность свойств безопасности информации может быть иной. Для открытой информации, ущерб от разглашения которой несущественен, важнейшими могут быть такие качества, как доступность, целостность или защищенность от неправомерного тиражирования. К примеру, для платежных (финансовых) документов самым важным является свойство их целостности (достоверности, неискаженности). Затем, по степени важности, следует свойство доступности (потеря платежного документа или задержка платежей может обходиться очень дорого). Требований к обеспечению конфиденциальности отдельных платежных документов может не предъявляется вообще.

Попытки подойти к решению вопросов защиты такой информации с позиций традиционного обеспечения только конфиденциальности, терпят провал. Основными причинами этого, на наш взгляд, являются узость существующего подхода к защите информации, отсутствие опыта и соответствующих проработок в плане обеспечения целостности и доступности информации, не являющейся конфиденциальной.

Развитие системы классификации информации по уровням требований к ее защищенности предполагает введение ряда степеней (градаций) требований по обеспечению каждого из свойств безопасности информации: доступности, целостности, конфиденциальности и защищенности от тиражирования. Пример градаций требований к защищенности:

- нет требований;
- низкие;
- средние;
- высокие;
- очень высокие.

Количество дискретных градаций и вкладываемый в них смысл могут различаться. Главное, чтобы требования к защищенности различных свойств информации указывались отдельно и достаточно конкретно (исходя из серьезности возможного наносимого субъектам информационных отношений ущерба от нарушения каждого из свойств безопасности информации).

В дальнейшем любой отдельный функционально законченный документ (некоторую совокупность знаков), содержащий определенные сведения, вне

зависимости от вида носителя, на котором он находится, будем называть ***информационным пакетом***.

К одному типу информационных пакетов будем относить пакеты (типовые документы), имеющие сходство по некоторым признакам (по структуре, технологии обработки, типу сведений и т.п.).

Задача состоит в определении реальных уровней заинтересованности (высокая, средняя, низкая, отсутствует) субъектов в обеспечении требований к защищенности каждого из свойств различных типов информационных пакетов, циркулирующих в АС.

Требования же к системе защиты АС в целом (методам и средствам защиты) должны определяться, исходя из требований к защищенности различных типов информационных пакетов, обрабатываемых в АС, и с учетом особенностей конкретных технологий их обработки и передачи (уязвимости).

В одну категорию объединяются типы информационных пакетов с равными приоритетами и уровнями требований к защищенности (степенью важности обеспечения их свойств безопасности : доступности, целостности и конфиденциальности).

Предлагаемый порядок определения требований к защищенности циркулирующей в системе информации представлен ниже:

1. Составляется общий перечень типов информационных пакетов, циркулирующих в системе (документов, таблиц). Для этого с учетом предметной области системы пакеты информации разделяются на типы по ее тематике, функциональному назначению, сходности технологии обработки и т.п. признакам.

На последующих этапах первоначальное разбиение информации (данных) на типы пакетов может уточняться с учетом требований к их защищенности.

2. Затем для каждого типа пакетов, выделенного в первом пункте, и каждого критического свойства информации (доступности, целостности, конфиденциальности) определяются (например, методом экспертных оценок):

- перечень и важность (значимость по отдельной шкале) субъектов, интересы которых затрагиваются при нарушении данного свойства информации;
- уровень наносимого им при этом ущерба (незначительный, малый, средний, большой, очень большой и т.п.)и соответствующий уровень требований к защищенности.

При определении уровня наносимого ущерба необходимо учитывать:

- стоимость возможных потерь при получении информации конкурентом;
- стоимость восстановления информации при ее утрате;

- затраты на восстановление нормального процесса функционирования АС и т.д.

Если возникают трудности из-за большого разброса оценок для различных частей информации одного типа пакетов, то следует пересмотреть деление информации на типы пакетов, вернувшись к предыдущему пункту методики.

3. Для каждого типа информационных пакетов с учетом значимости субъектов и уровней наносимого им ущерба устанавливается степень необходимой защищенности по каждому из свойств информации (при равенстве значимости субъектов выбирается максимальное значение уровня).

Пример оценки требований к защищенности некоторого типа информационных пакетов приведен в таблице 1.

Таблица 1.

Субъекты	Уровень ущерба по свойствам информации			
	Конфиденциальность	Целостность	Доступность	Защита от тиражирования
N 1	Нет	Средняя	Средняя	Нет
N 2	Высокая	Средняя	Средняя	Нет
N m	Низкая	Низкая	Низкая	Нет
В итоге	Высокая	Средняя	Средняя	Нет

Выводы

К определению основных понятий в области безопасности информационных технологий и общих целей защиты надо подходить с позиции защиты интересов и законных прав субъектов информационных отношений. Необходимо всегда помнить, что защищать надо именно субъектов информационных отношений, так как в конечном счете именно им, а не самой информации или системам ее обработки может наноситься ущерб. Иными словами, защита информации и систем ее обработки - вторичная задача. Главная задача - это защита интересов субъектов информационных отношений. Такая расстановка акцентов позволяет правильно определять требования к защищенности конкретной информации и систем ее обработки.

В соответствии с возможной заинтересованностью различных субъектов информационных отношений существует четыре основных способа нанесения им ущерба посредством разного рода воздействий на информацию и системы ее обработки:

- нарушение конфиденциальности (раскрытие) информации;
- нарушение целостности информации (ее полное или частичное уничтожение, искажение, фальсификация, дезинформация);

- нарушение (частичное или полное) работоспособности системы. Вывод из строя или неправомерное изменение режимов работы компонентов системы обработки информации, их модификация или подмена могут приводить к получению неверных результатов расчетов, отказам системы от потока информации (непризнанию одной из взаимодействующих сторон факта передачи или приема сообщений) и/или отказам в обслуживании конечных пользователей;
- несанкционированное тиражирование открытой информации (не являющейся конфиденциальной), например, программ, баз данных, разного рода документации, литературных произведений и т.д. в нарушение прав собственников информации, авторских прав и т.п. Информация, обладая свойствами материальных объектов, имеет такую особенность, как неисчерпаемость ресурса, что существенно затрудняет контроль за ее тиражированием.

Защищать АС (с целью защиты интересов субъектов информационных отношений) необходимо не только от несанкционированного доступа (НСД) к хранимой и обрабатываемой в них информации, но и от неправомерного вмешательства в процесс ее функционирования, нарушения работоспособности системы, то есть от любых несанкционированных действий. Защищать необходимо все компоненты АС: оборудование, программы, данные, персонал.

Механический перенос подходов к обеспечению безопасности субъектов информационных отношений из одной предметной области в другую, как правило, успеха не имеет. Причина этого - существенные различия интересов субъектов в разных предметных областях, в частности, различия в приоритетах свойств защищаемой информации и требований к характеристикам систем обработки информации.

Требования к уровню защищенности критичных свойств информационных пакетов различных типов (документов, справок, отчетов и т.п.) в конкретной предметной области должны устанавливаться ее владельцами (собственниками) или другими субъектами информационных отношений на основе анализа серьезности последствий нарушения каждого из свойств информации (типов информационных пакетов): доступности, целостности и конфиденциальности.

Прежде чем переходить к рассмотрению основных задач и подходов к построению систем защиты, призванных обеспечить надлежащий уровень безопасности субъектов информационных отношений, надо уточнить, от какого рода нежелательных воздействий необходимо защищать информацию и автоматизированные системы ее обработки и передачи.

2. УГРОЗЫ БЕЗОПАСНОСТИ АС

Одним из важнейших аспектов проблемы обеспечения безопасности компьютерных систем является определение, анализ и классификация возможных угроз безопасности АС. Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для проведения анализа риска и формулирования требований к системе защиты АС.

Особенности современных АС как объекта защиты

Как показывает анализ, большинство современных автоматизированных систем обработки информации в общем случае представляет собой территориально распределенные системы интенсивно взаимодействующих (синхронизирующихся) между собой по данным (ресурсам) и управлению (событиям) локальных вычислительных сетей (ЛВС) и отдельных ЭВМ.

В распределенных АС возможны все "традиционные" для локально расположенных (централизованных) вычислительных систем способы несанкционированного вмешательства в их работу и доступа к информации. Кроме того, для них характерны и новые специфические каналы проникновения в систему и несанкционированного доступа к информации, наличие которых объясняется целым рядом их особенностей.

Перечислим основные из особенностей распределенных АС:

- территориальная разнесенность компонентов системы и наличие интенсивного обмена информацией между ними;
- широкий спектр используемых способов представления, хранения и передачи информации;
- интеграция данных различного назначения, принадлежащих различным субъектам, в рамках единых баз данных и, наоборот, размещение необходимых некоторым субъектам данных в различных удаленных узлах сети;
- абстрагирование владельцев данных от физических структур и места размещения данных;
- использование режимов распределенной обработки данных;
- участие в процессе автоматизированной обработки информации большого количества пользователей и персонала различных категорий;
- непосредственный и одновременный доступ к ресурсам (в том числе и информационным) большого числа пользователей (субъектов) различных категорий;
- высокая степень разнородности используемых средств вычислительной техники и связи, а также их программного обеспечения;

- отсутствие специальной аппаратной поддержки средств защиты в большинстве типов технических средств, широко используемых в АС.

Уязвимость основных структурно-функциональных элементов распределенных АС

В общем случае АС состоят из следующих основных структурно-функциональных элементов:

- рабочих станций - отдельных ЭВМ или удаленных терминалов сети, на которых реализуются автоматизированные рабочие места пользователей (абонентов, операторов);
- серверов или Host машин (служб файлов, печати, баз данных и т.п.) не выделенных (или выделенных, то есть не совмещенных с рабочими станциями) высокопроизводительных ЭВМ, предназначенных для реализации функций хранения, печати данных, обслуживания рабочих станций сети и т.п. действий;
- межсетевых мостов (шлюзов, центров коммутации пакетов, коммуникационных ЭВМ) - элементов, обеспечивающих соединение нескольких сетей передачи данных, либо нескольких сегментов одной и той же сети, имеющих различные протоколы взаимодействия;
- каналов связи (локальных, телефонных, с узлами коммутации и т.д.).

Рабочие станции являются наиболее доступными компонентами сетей и именно с них могут быть предприняты наиболее многочисленные попытки совершения несанкционированных действий. С рабочих станций осуществляется управление процессами обработки информации, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На видеомониторы и печатающие устройства рабочих станций выводится информация при работе пользователей (операторов), выполняющих различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы. Именно поэтому рабочие станции должны быть надежно защищены от доступа посторонних лиц и содержать средства разграничения доступа к ресурсам со стороны законных пользователей, имеющих разные полномочия. Кроме того, средства защиты должны предотвращать нарушения нормальной настройки рабочих станций и режимов их функционирования, вызванные неумышленным вмешательством неопытных (невнимательных) пользователей.

В особой защите нуждаются такие привлекательные для злоумышленников элементы сетей как серверы (Host - машины) и мосты. Первые - как концентраторы больших объемов информации, вторые - как элементы, в которых осуществляется преобразование (возможно через открытую, нешифрованную форму представления) данных при согласовании протоколов обмена в различных участках сети.

Благоприятным для повышения безопасности серверов и мостов обстоятельством является, как правило, наличие возможностей по их надежной защите физическими средствами и организационными мерами в силу их выделенности, позволяющей сократить до минимума число лиц из персонала сети, имеющих непосредственный доступ к ним. Иными словами, непосредственные случайные воздействия персонала и преднамеренные воздействия злоумышленников на выделенные серверы и мосты можно считать маловероятными. В то же время, надо ожидать массированной атаки на серверы и мосты с использованием средств удаленного доступа. Здесь злоумышленники прежде всего могут искать возможности повлиять на работу различных подсистем серверов и мостов, используя недостатки протоколов обмена и средств разграничения удаленного доступа к ресурсам и системным таблицам. Использоваться могут все возможности и средства, от стандартных (без модификации компонентов) до подключения специальных аппаратных средств (каналы, как правило, слабо защищены от подключения) и применения высококлассных программ для преодоления системы защиты.

Конечно, сказанное выше не означает, что не будет попыток внедрения аппаратных и программных закладок в сами мосты и серверы, открывающих дополнительные широкие возможности по несанкционированному удаленному доступу. Закладки могут быть внедрены как с удаленных станций (посредством вирусов или иным способом), так и непосредственно в аппаратуру и программы серверов при их ремонте, обслуживании, модернизации, переходе на новые версии программного обеспечения, смене оборудования.

Каналы и средства связи также нуждаются в защите. В силу большой пространственной протяженности линий связи (через неконтролируемую или слабо контролируемую территорию) практически всегда существует возможность подключения к ним, либо вмешательства в процесс передачи данных. Возможные при этом угрозы подробно изложены ниже.

Угрозы безопасности информации, АС и субъектов информационных отношений

Под угрозой (вообще) обычно понимают *потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.*

Угрозой интересам субъектов информационных отношений будем называть потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или другие компоненты АС может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

В силу особенностей современных АС, перечисленных выше, существует значительное число различных видов угроз безопасности субъектов информационных отношений.

Нарушением безопасности (или просто нарушением) будем называть реализацию угрозы безопасности.

В настоящей работе предпринята попытка возможно более полного охвата угроз безопасности субъектов информационных отношений. Однако следует иметь ввиду, что научно-технический прогресс может привести к появлению принципиально новых видов угроз и что изощренный ум злоумышленника способен придумать новые способы преодоления систем безопасности, НСД к данным и дезорганизации работы АС.

Основные виды угроз безопасности субъектов информационных отношений

Основными видами угроз безопасности АС и информации (угроз интересам субъектов информационных отношений) являются:

- стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.);
- сбои и отказы оборудования (технических средств) АС;
- последствия ошибок проектирования и разработки компонентов АС (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.);
- ошибки эксплуатации (пользователей, операторов и другого персонала);
- преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.п.).

Классификация угроз безопасности

Все множество потенциальных угроз по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные) (рис.2.1).

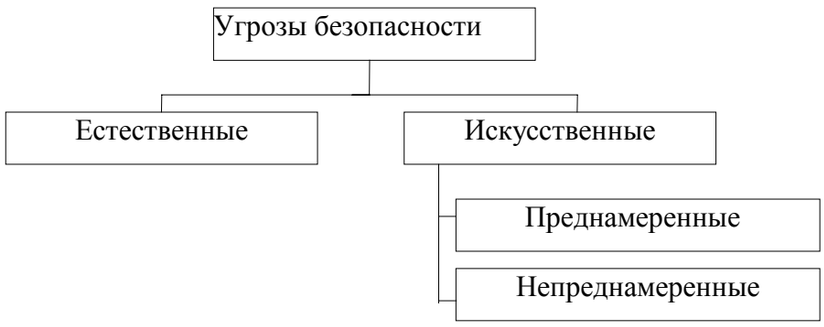


Рис. 2.1.

Естественные угрозы - это угрозы, вызванные воздействиями на АС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы - это угрозы АС, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

- ***непреднамеренные (неумышленные, случайные) угрозы***, вызванные ошибками в проектировании АС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;
- ***преднамеренные (умышленные) угрозы***, связанные с корыстными устремлениями людей (злоумышленников).

Источники угроз по отношению к АС могут быть внешними или внутренними (компоненты самой АС - ее аппаратура, программы, персонал).

Основные непреднамеренные искусственные угрозы

Основные непреднамеренные искусственные угрозы АС (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

1) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

2) неправомерное отключение оборудования или изменение режимов работы устройств и программ;

3) неумышленная порча носителей информации;

4) запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

5) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

6) заражение компьютера вирусами;

7) неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;

8) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);

9) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

10) игнорирование организационных ограничений (установленных правил) при работе в системе;

11) вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);

12) некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;

13) пересылка данных по ошибочному адресу абонента (устройства);

14) ввод ошибочных данных;

15) неумышленное повреждение каналов связи.

Основные преднамеренные искусственные угрозы

Основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

1) физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);

2) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

3) действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);

4) внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);

5) вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;

6) применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;

7) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);

8) перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

9) хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ);

10) несанкционированное копирование носителей информации;

11) хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);

12) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

13) чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования;

14) незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя ("маскарад");

15) несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;

16) вскрытие шифров криптозащиты информации;

17) внедрение аппаратных спецвложений, программных "закладок" и "вирусов" ("троянских коней" и "жучков"), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;

18) незаконное подключение к линиям связи с целью работы "между строк", с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;

19) незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

Классификация каналов проникновения в систему и утечки информации

Все каналы проникновения в систему и утечки информации разделяют на прямые и косвенные. Под косвенными понимают такие каналы, использование которых не требует проникновения в помещения, где расположены компоненты системы. Для использования прямых каналов такое проникновение необходимо. Прямые каналы могут использоваться без внесения изменений в компоненты системы или с изменениями компонентов [22].

По типу основного средства, используемого для реализации угрозы все возможные каналы можно условно разделить на три группы, где таковыми средствами являются: человек, программа или аппаратура.

Классификация видов нарушений работоспособности систем и несанкционированного доступа к информации по объектам воздействия и способам нанесения ущерба безопасности приведена в таблице 2.

По способу получения информации потенциальные каналы доступа можно разделить на :

- физический;
- электромагнитный (перехват излучений);
- информационный (программно-математический).

При контактном НСД (физическом, программно-математическом) возможные угрозы информации реализуются путем доступа к элементам АС, к

носителям информации, к самой вводимой и выводимой информации (и результатам), к программному обеспечению (в том числе к операционным системам), а также путем подключения к линиям связи.

При бесконтактном доступе (например, по электромагнитному каналу) возможные угрозы информации реализуются перехватом излучений аппаратуры АС, в том числе наводимых в токопроводящих коммуникациях и цепях питания, перехватом информации в линиях связи, вводом в линии связи ложной информации, визуальным наблюдением (фотографированием) устройств отображения информации, прослушиванием переговоров персонала АС и пользователей.

Таблица 2

Способы нанесения ущерба	Объекты воздействий			
	Оборудование	Программы	Данные	Персонал
Раскрытие (утечка) информации	Хищение носителей информации, подключение к линии связи, несанкционированное использование ресурсов	Несанкционированное копирование перехват	Хищение, копирование, перехват	Передача сведений о защите, разглашение, халатность
Потеря целостности информации	Подключение, модификация, спец.вложения, изменение режимов работы, несанкционированное использование ресурсов	Внедрение “троянских коней” и “жучков”	Искажение, модификация	Вербовка персонала, “маскарад”
Нарушение работоспособности автоматизированной системы	Изменение режимов функционирования, вывод из строя, хищение, разрушение	Искажение, удаление, подмена	Искажение, удаление, навязывание ложных данных	Уход, физическое устранение
Незаконное тиражирование (воспроизведение) информации	Изготовление аналогов без лицензий	Использование незаконных копий	Публикация без ведома авторов	

Преступления, в том числе и компьютерные, совершаются людьми. Пользователи системы и ее персонал, с одной стороны, являются составной частью, необходимым элементом АС. С другой стороны, они же являются основной причиной и движущей силой нарушений и преступлений. В этом

смысле вопросы безопасности автоматизированных систем есть суть вопросы человеческих отношений и человеческого поведения.

Неформальная модель нарушителя в АС

Нарушитель - это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленником будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п. Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. Исследовав причины нарушений, можно либо повлиять на сами эти причины (конечно если это возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлений.

В каждом конкретном случае, исходя из конкретной технологии обработки информации, может быть определена модель нарушителя, которая должна быть адекватна реальному нарушителю для данной АС.

При разработке модели нарушителя определяются:

- предположения о категориях лиц, к которым может принадлежать нарушитель;
- предположения о мотивах действий нарушителя (преследуемых нарушителем целях);
- предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);
- ограничения и предположения о характере возможных действий нарушителей.

По отношению к АС нарушители могут быть внутренними (из числа персонала системы) или внешними (посторонними лицами). Внутренним нарушителем может быть лицо из следующих категорий персонала:

- пользователи (операторы) системы;
- персонал, обслуживающий технические средства (инженеры, техники);
- сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты);

- технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты АС);
- сотрудники службы безопасности АС;
- руководители различных уровней должностной иерархии.

Посторонние лица, которые могут быть нарушителями:

- клиенты (представители организаций, граждане);
- посетители (приглашенные по какому-либо поводу);
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.);
- представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;
- лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность АС);
- любые лица за пределами контролируемой территории.

Можно выделить три основных мотива нарушений: безответственность, самоутверждение и корыстный интерес.

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.

Некоторые пользователи считают получение доступа к системным наборам данных крупным успехом, затевая своего рода игру "пользователь - против системы" ради самоутверждения либо в собственных глазах, либо в глазах коллег.

Нарушение безопасности АС может быть вызвано и корыстным интересом пользователя системы. В этом случае он будет целенаправленно пытаться преодолеть систему защиты для доступа к хранимой, передаваемой и обрабатываемой в АС информации. Даже если АС имеет средства, делающие такое проникновение чрезвычайно сложным, полностью защитить ее от проникновения практически невозможно.

Всех нарушителей можно классифицировать следующим образом.

По уровню знаний об АС :

- знает функциональные особенности АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами;

- обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;
- обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;
- знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

По уровню возможностей (используемым методам и средствам):

- применяющий чисто агентурные методы получения сведений;
- применяющий пассивные средства (технические средства перехвата без модификации компонентов системы);
- использующий только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны;
- применяющий методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

По времени действия:

- в процессе функционирования АС (во время работы компонентов системы);
- в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т.п.);
- как в процессе функционирования АС, так и в период неактивности компонентов системы.

По месту действия:

- без доступа на контролируемую территорию организации;
- с контролируемой территории без доступа в здания и сооружения;
- внутри помещений, но без доступа к техническим средствам АС;
- с рабочих мест конечных пользователей (операторов) АС;
- с доступом в зону данных (баз данных, архивов и т.п.);

- с доступом в зону управления средствами обеспечения безопасности АС.

Могут учитываться следующие ограничения и предположения о характере действий возможных нарушителей:

- работа по подбору кадров и специальные мероприятия затрудняют возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий по преодолению подсистемы защиты двух и более нарушителей;
- нарушитель, планируя попытки НСД, скрывает свои несанкционированные действия от других сотрудников;
- НСД может быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки информации и т.д.

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов его облика. Каждый вид нарушителя должен быть охарактеризован значениями характеристик, приведенных выше.

Выводы

Специфика распределенных АС, с точки зрения их уязвимости, связана в основном с наличием интенсивного информационного взаимодействия между территориально разнесенными и разнородными (разнотипными) элементами.

Уязвимыми являются буквально все основные структурно-функциональные элементы распределенных АС: рабочие станции, серверы (Host-машины), межсетевые мосты (шлюзы, центры коммутации), каналы связи.

Защищать компоненты АС необходимо от всех видов воздействий: стихийных бедствий и аварий, сбоев и отказов технических средств, ошибок персонала и пользователей, ошибок в программах и от преднамеренных действий злоумышленников.

Имеется широчайший спектр вариантов путей преднамеренного или случайного несанкционированного доступа к данным и вмешательства в процессы обработки и обмена информацией (в том числе, управляющей согласованным функционированием различных компонентов сети и разграничением ответственности за преобразование и дальнейшую передачу информации).

Правильно построенная (адекватная реальности) модель нарушителя, в которой отражаются его практические и теоретические возможности, априорные знания, время и место действия и т.п. характеристики - важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

3. ОСНОВНЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ БЕЗОПАСНОСТИ, ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ, ОСНОВНЫЕ МЕХАНИЗМЫ ЗАЩИТЫ

Целью данного раздела является анализ основных известных мер противодействия угрозам безопасности АС, обзор технических и организационно-технических мер, методов и средств противодействия, а также формулирование основных принципов построения комплексной системы защиты информации.

Задачи системы компьютерной безопасности

По результатам проведенного анализа возможных угроз АС можно сформулировать перечень основных задач, которые должны решаться системой компьютерной безопасности:

- управление доступом пользователей к ресурсам АС с целью ее защиты от неправомерного случайного или умышленного вмешательства в работу системы и несанкционированного (с превышением предоставленных полномочий) доступа к ее информационным, программным и аппаратным ресурсам со стороны посторонних лиц, а также лиц из числа персонала организации и пользователей;
- защита данных, передаваемых по каналам связи;
- регистрация, сбор, хранение, обработка и выдача сведений обо всех событиях, происходящих в системе и имеющих отношение к ее безопасности;
- контроль работы пользователей системы со стороны администрации и оперативное оповещение администратора безопасности о попытках несанкционированного доступа к ресурсам системы;
- контроль и поддержание целостности критичных ресурсов системы защиты и среды исполнения прикладных программ;
- обеспечение замкнутой среды проверенного программного обеспечения с целью защиты от бесконтрольного внедрения в систему потенциально опасных программ (в которых могут содержаться вредоносные закладки или опасные ошибки) и средств преодоления системы

защиты, а также от внедрения и распространения компьютерных вирусов;

- управление средствами системы защиты.

Обычно различают внешнюю и внутреннюю безопасность компьютерных систем. Внешняя безопасность включает защиту АС от стихийных бедствий (пожар, наводнение и т.п.) и от проникновения в систему злоумышленников извне с целями хищения, получения доступа к информации или вывода системы из строя. В данной работе меры и методы защиты АС от стихийных бедствий и аварий, а также меры физической защиты (охраны и др.) не рассматриваются.

Все усилия по обеспечению внутренней безопасности компьютерных систем фокусируются на создании надежных и удобных механизмов регламентации деятельности всех ее законных пользователей и обслуживающего персонала для принуждения их к безусловному соблюдению установленной в организации дисциплины доступа к ресурсам системы (в том числе к информации).

Меры противодействия угрозам безопасности. Классификация мер обеспечения безопасности компьютерных систем

По способам осуществления все меры обеспечения безопасности компьютерных систем подразделяются на: правовые (законодательные), морально-этические, организационные (административные), физические и технические (аппаратурные и программные) [6,22].

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

К морально-этическим мерам противодействия относятся 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 нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

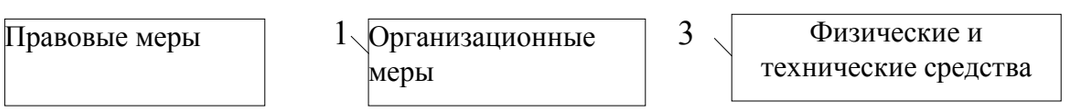
Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени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

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных;
- мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности);
- мероприятия, осуществляемые при подборе и подготовке персонала системы;
- организацию охраны и надежного пропускного режима;
- организацию учета, хранения, использования и уничтожения документов и носителей с информацией;
- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);
- организацию явного и скрытого контроля за работой пользователей;
- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения и т.п.

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав АС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

Взаимосвязь рассмотренных выше мер обеспечения безопасности приведена на рис.3.1.



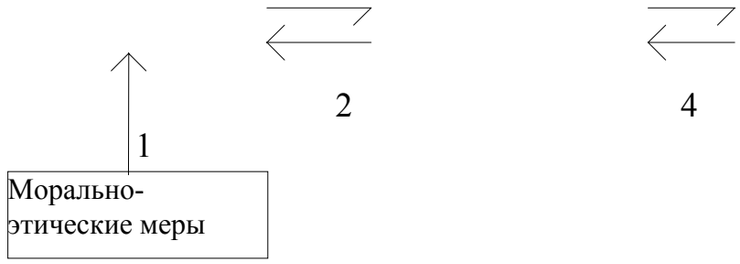


Рис. 3.1

1 - Организационные меры обеспечивают исполнение существующих нормативных актов и строятся с учетом существующих правил поведения, принятых в стране и/или организации

2 - Воплощение организационных мер требует создания нормативных документов

3 - Для эффективного применения организационные меры должны быть поддержаны физическими и техническими средствами

4 - Применение и использование технических средств защиты требует соответствующей организационной поддержки.

Достоинства и недостатки различных мер защиты

Законодательные и морально-этические меры

Эти меры определяют правила обращения с информацией и ответственность субъектов информационных отношений за их соблюдение.

Законодательные и морально-этические меры противодействия, являются универсальными в том смысле, что принципиально применимы для всех каналов проникновения и НСД к АС и информации. В некоторых случаях они являются единственно применимыми, как например, при защите открытой информации от незаконного тиражирования или при защите от злоупотреблений служебным положением при работе с информацией. Подробнее эти меры рассмотрены в [3].

Организационные меры

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

Организационные меры играют значительную роль в обеспечении безопасности компьютерных систем.

Организационные меры - это единственное, что остается, когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый

уровень безопасности. Однако, это вовсе не означает, что систему защиты необходимо строить исключительно на их основе , как это часто пытаются сделать чиновники, далекие от технического прогресса. Этим мерам присущи серьезные недостатки, такие как:

- низкая надежность без соответствующей поддержки физическими, техническими и программными средствами (люди склонны к нарушению любых установленных дополнительных ограничений и правил, если только их можно нарушить);
- дополнительные неудобства, связанные с большим объемом рутинной формальной деятельности.

Организационные меры необходимы для обеспечения эффективного применения других мер и средств защиты в части, касающейся регламентации действий людей. В то же время организационные меры необходимо поддерживать более надежными физическими и техническими средствами.

Более подробно организационные меры рассмотрены в главе 4.

Физические и технические средства защиты

Физические и технические средства защиты призваны устранить недостатки организационных мер, поставить прочные барьеры на пути злоумышленников и в максимальной степени исключить возможность неумышленных (по ошибке или халатности) нарушений персонала и пользователей системы.

Рассмотрим известное утверждение о том, что создание абсолютной (то есть идеально надежной) системы защиты принципиально невозможно.

Даже при допущении возможности создания абсолютно надежных физических и технических средств защиты, перекрывающих все каналы, которые необходимо перекрыть, всегда остается возможность воздействия на персонал системы, осуществляющий необходимые действия по обеспечению корректного функционирования этих средств (администратора АС, администратора безопасности и т.п.). Вместе с самими средствами защиты эти люди образуют так называемое "ядро безопасности". В этом случае, стойкость системы безопасности будет определяться стойкостью персонала из ядра безопасности системы, и повышать ее можно только за счет организационных (кадровых) мероприятий, законодательных и морально-этических мер. Но даже имея совершенные законы и проводя оптимальную кадровую политику, все равно проблему защиты до конца решить не удастся. Во-первых, потому, что вряд ли удастся найти персонал, в котором можно было быть абсолютно уверенным, и в отношении которого невозможно было бы предпринять действий, вынуждающих его нарушить запреты. Во-вторых, даже абсолютно надежный человек может допустить случайное, неумышленное нарушение.

Основные принципы построения систем защиты АС

Защита информации в АС должна основываться на следующих основных принципах:

- системности;
- комплексности;
- непрерывности защиты;
- разумной достаточности;
- гибкости управления и применения;
- открытости алгоритмов и механизмов защиты;
- простоты применения защитных мер и средств.

Принцип системности

Системный подход к защите компьютерных систем предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности АС.

При создании системы защиты необходимо учитывать все слабые, наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Принцип комплексности

В распоряжении специалистов по компьютерной безопасности имеется широкий спектр мер, методов и средств защиты компьютерных систем. Комплексное их использование предполагает согласованное применение

разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонированно. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одной из наиболее укрепленных линий обороны призваны быть средства защиты, реализованные на уровне операционных систем (ОС) в силу того, что ОС - это как раз та часть компьютерной системы, которая управляет использованием всех ее ресурсов. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж обороны.

Принцип непрерывности защиты

Защита информации - это не разовое мероприятие и даже не определенная совокупность проведенных мероприятий и установленных средств защиты, а ***непрерывный целенаправленный процесс***, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.

Разработка системы защиты должна вестись параллельно с разработкой самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, позволит создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

Разумная достаточность

Создать абсолютно непреодолимую систему защиты принципиально невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту. Поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть мощности и ресурсов компьютерной системы и может создавать ощутимые дополнительные не-

удобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Гибкость системы защиты

Часто приходится создавать систему защиты в условиях большой неопределенности. Поэтому принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Естественно, что для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются. В таких ситуациях свойство гибкости спасает владельцев АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже автору). Однако, это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна.

Принцип простоты применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Основные механизмы защиты компьютерных систем от проникновения с целью дезорганизации их работы и НСД к информации

Определим ряд понятий, необходимых в дальнейшем.

Объект - пассивный компонент системы, единица ресурса автоматизированной системы (устройство, диск, каталог, файл и т.п.), доступ к которому регламентируется правилами разграничения доступа.

Субъект - активный компонент системы (пользователь, процесс, программа), действия которого регламентируются правилами разграничения доступа.

Доступ к информации - ознакомление с информацией (копирование, тиражирование), ее модификация (корректировка) или уничтожение (удаление).

Доступ к ресурсу - получение субъектом возможности манипулировать (использовать, управлять, изменять характеристики и т.п.) данным ресурсом.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе.

Разграничение доступа к ресурсам АС - это такой порядок использования ресурсов автоматизированной системы, при котором субъекты получают доступ к объектам в строгом соответствии с установленными правилами.

Авторизованный субъект доступа - субъект, которому предоставлены соответствующие права доступа к объектам системы (полномочия).

Несанкционированный доступ (НСД) - доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа.

Несанкционированное действие - действие субъекта в нарушение установленных в системе правил обработки информации.

Для реализации приведенных выше мер защиты компьютерных систем используются универсальные механизмы защиты информации [6].

К числу таких механизмов относятся:

- идентификация (именование и опознавание), аутентификация (подтверждение подлинности) и авторизация (присвоение полномочий) субъектов;
- контроль (разграничение) доступа к ресурсам системы;
- регистрация и анализ событий, происходящих в системе;
- контроль целостности ресурсов системы.

Механизмы идентификации, аутентификации и авторизации необходимы для подтверждения подлинности субъекта, обеспечения его работы в системе, и определения законности прав субъекта на данный объект или на определенные действия с ним.

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

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

Авторизация - это предоставление субъекту прав на доступ к объекту.

Под ***контролем доступа*** будем понимать ограничение возможностей использования ресурсов системы программами, процессами или другими системами (для сети) в соответствии с правилами разграничения доступа.

Основным объектом внимания средств контроля доступа являются совместно используемые 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 доступа субъектов к совместно используемым объектам:

- ***Физическое*** - субъекты обращаются к физически различным объектам (однотипным устройствам, наборам данных на разных носителях и т.д.).
- ***Временное*** - субъекты с различными правами доступа к объекту получают его в различные промежутки времени.
- ***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.
- ***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 доступа, они могут иметь разную реализацию в различных средствах защиты.

Механизм регистрации обеспечивает получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля, а также регистрацию действий, признанных администрацией АС потенциально опасными для безопасности системы. Анализ собранной информации позволяет выявить средства и априорную информацию, использованные нарушителем при воздействии на систему и определить, как далеко зашло нару-

шение, подсказать метод его расследования и способы исправления ситуации.

Механизм контроля целостности ресурсов системы предназначен для своевременного обнаружения модификации ресурсов системы. Это позволяет обеспечить правильность функционирования системы защиты и целостность обрабатываемой информации.

Эти универсальные механизмы защиты могут применяться в различных вариациях и совокупностях в конкретных методах и средствах защиты. Стоит отметить, что наибольший эффект достигается при использовании всех механизмов.

Модели управления доступом •

Успех в достижении высокой степени безопасности АС зависит от тщательности разработки и реализации управления имеющимися в системе механизмами безопасности. Как показывает практика, наилучшие результаты в создании безопасных систем достигаются в том случае, когда разработчики системы учитывают требования безопасности уже на этапе формулирования целей разработки и самых общих принципов построения системы. При этом разработчики должны четко понимать суть требований безопасности.

В таком случае, разрабатываемая система может быть небезопасной в силу одной из двух причин :

- есть ошибки в реализации механизмов защиты или механизмов управления ими;
- ошибочно, недостаточно полно, или неверно понято само определение того, что значит в отношении системы выражение "быть безопасной".

Для устранения первой причины необходимо применение современных технологий создания программного обеспечения в сочетании с принципами разработки, специфичными для выполнений требований безопасности.

Для устранения второй причины необходимо как можно точнее сформулировать понятие "быть безопасной" в отношении разрабатываемой системы.

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

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

• Материал по моделям управления доступом подготовлен И.Э. Моисеенковым

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

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

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

Нисходящий метод разработки системы обеспечения безопасности может быть неформальным или формальным (Рис.3.2.).

Рис.3.2.

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

По мере увеличения сложности системы взаимосвязи ее компонентов становятся все менее очевидными; становится сложно описать эти взаимосвязи с достаточной степенью точности некоторым неформальным образом (например, на естественном языке). При разработке систем обеспечения

безопасности точность в описании компонентов и их взаимосвязей является едва ли не решающим условием достижения успеха, поэтому для обеспечения надлежащей степени точности применяется строгий аппарат формальной математики, что и составляет суть формального метода разработки.

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

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

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

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

Модель позволяет провести анализ свойств системы, но не накладывает ограничений на реализацию тех или иных механизмов защиты. Так как модель является формальной, возможно осуществить доказательство различных свойств безопасности всей системы.

Моделирование требует значительных усилий и дает хорошие результаты только при наличии времени и ресурсов. Если система уже создана и имеется возможность сделать лишь отдельные изменения в отдельных местах существующей системы ("залатать дыры"), в любом случае маловероятно значительное улучшение состояния безопасности системы и моделирование поэтому будет непродуктивным занятием.

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

Типы моделей управления доступом

Модель конечного автомата описывает систему как абстрактную математическую машину. В этой модели переменные состояния представляют состояния машины, а функции перехода описывают способ изменения переменных.

Напомним, что модель управления доступом имеет дело только с наиболее существенными переменными состояния, влияющими на безопасность, и потому намного проще, чем полная модель конечного автомата для данной системы.

Модель матрицы доступа (Harrison, Ruzo и Ullman 1976) это частный случай реализации модели машины состояний. Состояния безопасности системы представлены в виде таблицы, содержащей по одной строке для каждого субъекта системы и по одной колонке для каждого субъекта и объекта (таблица 3). Каждое пересечение в массиве определяет режим доступа данного субъекта к каждому объекту или другому субъекту системы.

Таблица 3

Субъекты	Объекты			Субъекты		
	1	2	3	1	2	3
1	Чтение Запись	Чтение		---------	Запись	Пересылка
2	Чтение	Чтение Исполнение	Чтение Запись	Пересылка	---------	
3		Чтение Запись	Исполнение	Пересылка	Запись	---------

Второй составляющей модели матрицы доступа является набор функций перехода, описывающих способ изменения матрицы доступа.

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

Другим способом описания управления доступом является модель, выраженная в терминах ***меток безопасности***, приписываемых субъектам и объектам системы. Режим доступа, которым обладает субъект по отношению к объекту, определяется при сравнении их меток безопасности, вместо того, чтобы искать соответствующее пересечение строки и столбца в матрице доступа. Модель может использовать как матрицу доступа, так и атрибуты безопасности. Все подобные модели, рассматривающие доступ субъекта к объекту, могут быть названы ***моделями управления доступом.***

Вариантом модели управления доступом является ***модель информационных потоков (***Denning, 1983), которая предназначена для анализа потоков информации из одного объекта в другой на основании их меток безопасности

Еще одним типом модели является ***модель интерференции***, в которой субъекты, работающие в различных доменах, защищены от взаимовлияния друг на друга любым способом, нарушающим свойства безопасности системы (Goguen и Meseguer, 1982).

Характеристики модели безопасности

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

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

Описание модели управления доступом в системе как конечного автомата

Представления модели управления доступом как конечного автомата получили предпочтение из-за того, что они представляют компьютерную систему способом, имитирующим работу операционной системы и аппаратуры. Переменная состояния является абстракцией для каждого бита и байта в системе, изменяющихся по мере работы системы. Функции переходов из состояния в состояние - это абстракция обращений к операционной системе, явно описывающие то, как состояние может (или не может) изменяться.

Модель управления доступом работает не со всеми переменными состояния и функциями системы. Выбор для моделирования переменных и функций, имеющих отношение к безопасности, остается за разработчиком модели.

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

Таким образом в разработке модели управления доступом можно выделить следующие шаги:

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

2. Определение условий для безопасного состояния. Это определение является выражением отношений между значениями переменных состояния, истинность которого должна обеспечиваться при переходах состояния.

3. Определение функций переходов из состояния в состояние. Эти функции описывают допустимые способы изменения переменных состояния. Они также называются правилами изменения доступа, поскольку их цель состоит в указании изменений, которые может производить система, а вовсе не в определении всех возможных изменений. Правила могут быть очень общими и могут допускать наличие функций, которых нет в реальной системе, однако система не может менять переменные состояния каким-либо способом, который не допускается функциями.

Можно выделить несколько характерных черт функций перехода:

- назначение функции - определение взаимосвязи между переменными в предыдущем и новом состояниях;
- функция не задает какого-либо конкретного порядка в выполнении алгоритма операции. Иными словами, функция может рассматриваться как определение того, что произойдет с состоянием по завершении операции;
- функция элементарна. Это значит, что ее эффект не разделяем на более мелкие действия и не прерываем. Указанное изменение состояния происходит моментально, т.е. какого-либо промежутка времени, "в течение" которого происходил бы переход состояния, определить невозможно.

Следует помнить, что каждая дополнительная переменная состояния и сопутствующие ей операции существенно усложняют как саму модель, так и доказательство ее свойств. Модель управления доступом предполагает представление только поведения системы, связанного с безопасностью.

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

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

6. Доказывается, что начальное состояние безопасно в соответствии с определением.

Модель безопасности Белл–Ла Падула

Одна из первых моделей безопасности - и впоследствии наиболее часто используемой - была разработана Дэвидом Беллом и Леонардо Ла Падула для моделирования работы компьютера.

Рассмотрим систему из двух файлов и двух процессов (рис.3.3). Один файл и один процесс являются ***несекретными***, другой файл и процесс - ***секретными***.

Простое правило безопасности предотвращает чтение ***секретного*** файла ***несекретным*** процессом. Оба процесса могут читать и записывать данные в ***несекретный*** файл. Однако, легко может произойти нарушение правил управления доступом, если ***секретный*** процесс считает информацию из ***секретного*** файла и запишет ее в ***несекретный*** файл. Это эквивалентно неавторизованному уменьшению класса доступа информации, хотя при этом не изменяется класс доступа ни одного файла.

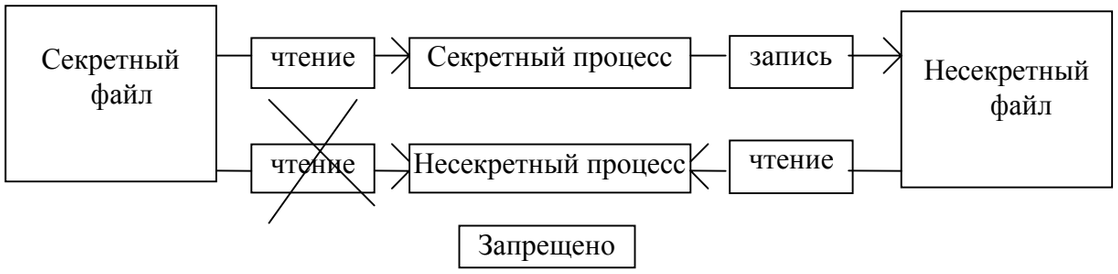


Рис.3.3.

Когда процесс записывает информацию в файл, класс доступа которого меньше, чем класс доступа процесса, имеет место так называемый процесс записи вниз. Ограничение, направленное на исключение нисходящей записи получило в модели Белл–Ла Падула название ****-свойства*** или ***свойства ограничения.***

Таким образом, модель многоуровневой безопасности имеет два основных свойства:

- ***простая безопасность***: субъект может только читать объект, если класс доступа субъекта доминирует над классом доступа объекта. Другими словами, субъект может читать "вниз", но не может читать "вверх";
- ***свойство ограничения***: субъект может только записать в объект, если класс доступа субъекта превосходит класс доступа объекта. Субъект может записывать "вверх", но не может записать "вниз".

Процесс не может ни читать объект с высшим классом доступа (свойство простой безопасности), ни записать объект с низшим классом доступа (*-свойство или свойство ограничения) (рис.3.4).

При формализации многоуровневого управления безопасностью, модель Белл–Ла Падула определяет структуру класса доступа и устанавливает упорядочивание отношений между классами доступа (доминирование). Кроме того определяются два уникальных класса доступа: ***SYSTEM HIGH***, который превосходит все остальные классы доступа, и ***SYSTEM LOW***, который превосходят все другие классами. Изменения классов доступа в рамках модели Белл–Ла Падула не допускаются.

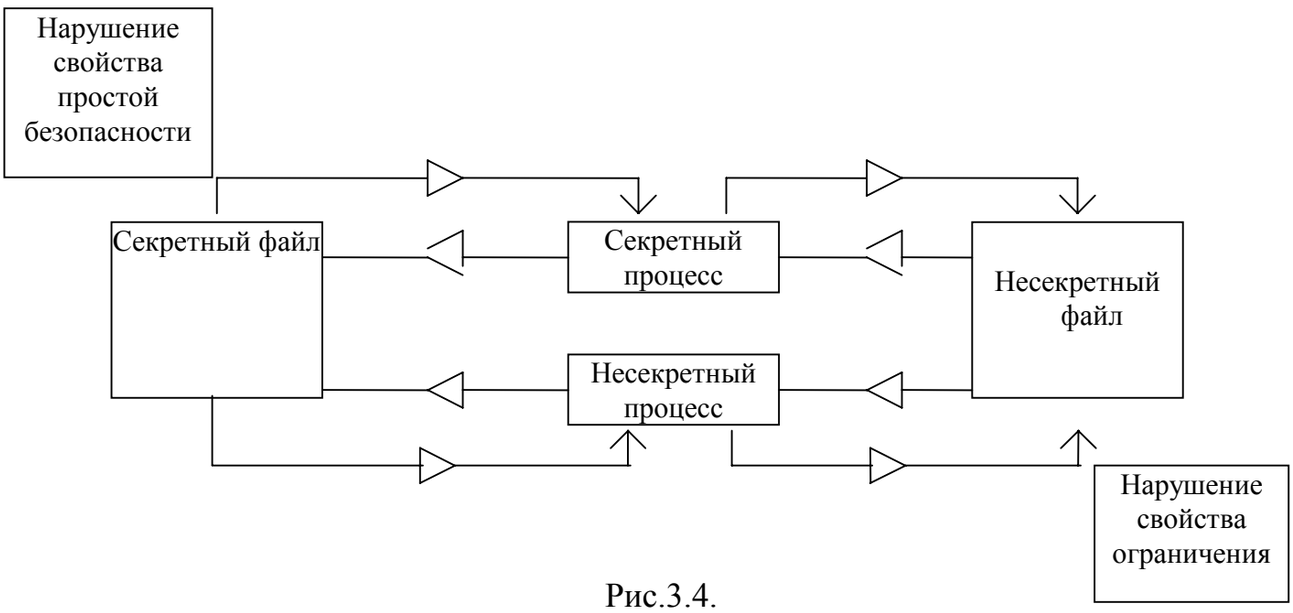


Рис.3.4.

Управление доступом в модели Белл–Ла Падула происходит как с использованием матрицы управления доступом, так и с использованием меток безопасности и ранее приведенных правил простой безопасности и свойства ограничения.

В дополнение к имеющимся режимам доступа чтения и записи, матрица управления доступом включает режимы добавления, исполнения и управления - причем последний определяет, может ли субъект передавать другим субъектам права доступа, которыми он обладает по отношению к объекту.

Управление при помощи меток безопасности усиливает ограничение предоставляемого доступа на основе сравнения атрибутов класса доступа субъектов и объектов.

В модели Белл–Ла Падула определено около двадцати функций (правил операций), выполняемых при модификации компонентов матрицы доступа, при запросе и получении доступа к объекту (например при открытии файла), создании и удалении объектов; при этом для каждой функции доказывается сохранение ею, в соответствии с определением, безопасного состояния. Лишь немногие разработки безопасных систем использовали функции, предложенные Белл и Ла Падула, чаще использовались собственные функции, разработанные на основе функций модели Белл–Ла Падула. Поэтому в настоящее время, когда говорят о модели Белл–Ла Падула, имеются в виду только простое условие безопасности и свойство ограничения, а не функции, составляющие основу модели, и их доказательства.

Анализ информационных потоков

Помимо выполнения основной своей задачи - математически точного представления требований правил управления доступом, модель управления доступом используется в процессе разработки системы для выполнения так называемого анализа информационного потока. Анализ информационного потока - это общая технология для анализа путей утечки информации в системе (Lampson, 1973; Denning, 1983); она применима к любой модели безопасности.

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

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

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

Следует учитывать, что формальный анализ потока - занятие весьма трудоемкое, поскольку проверяется каждая ссылка на каждую переменную состояния в модели. Анализ потока нельзя считать полноценным без рас-

смотрения каждой переменной, поскольку очень легко упустить скрытый канал именно через переменную, выпавшую из рассмотрения. Правила для определения возможности информационного потока сложны и трудны для применения вручную.

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

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

Поскольку существуют строгие правила и методы определения потенциальных потоков, их синтаксического анализа и доказательства допустимости, иногда говорят о модели информационного потока (см.выше), что представляется не совсем верным, поскольку формальная модель безопасности имеет собственное назначение помимо того, чтобы служить основой для проведения анализа информационного потока.

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

В более полном варианте метод формальной разработки включает также этап создания ***формальной спецификации***. Спецификация отличается от модели тем, что помимо переменных и функций, относящихся к обеспечению безопасности, описывает переменные и функции, реализующие в системе иные задачи. При этом следует отметить, что соответствие формальной спецификации разработанной ранее модели безопасности строго доказывается.

Системы разграничения доступа

Основную роль в обеспечении внутренней безопасности компьютерных систем выполняют системы управления доступом (разграничения доступа) субъектов к объектам доступа, реализующие концепцию единого диспетчера доступа (в английском варианте "reference monitor"- дословно, монитор ссылок).

Диспетчер доступа

Сущность концепции диспетчера доступа состоит в том, что некоторый абстрактный механизм является посредником при всех обращениях субъектов к объектам (Рис.3.5).

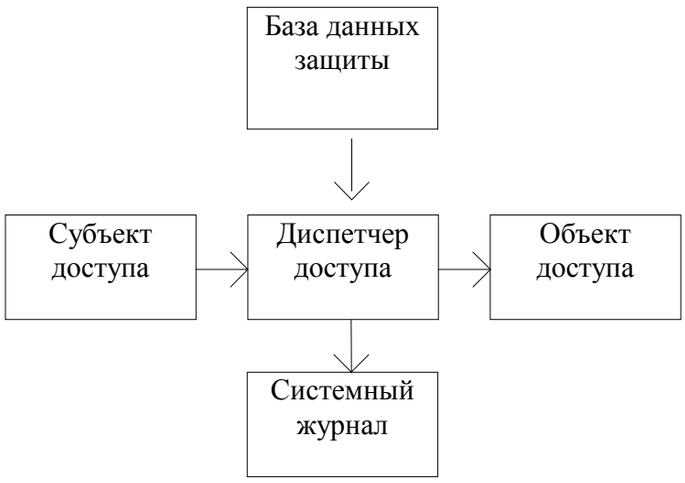


Рис. 3.5.

Диспетчер доступа должен выполнять следующие функции:

- проверять права доступа каждого субъекта к любому объекту на основании информации, содержащейся в базе данных защиты (правил разграничения доступа);
- при необходимости регистрировать факт доступа и его параметры в системном журнале.

Основными требованиями к реализации диспетчера доступа являются:

- требование полноты контролируемых операций, согласно которому проверке должны подвергаться все операции всех субъектов над всеми объектами системы. Обход диспетчера предполагается невозможным;
- требование изолированности, то есть защищенности диспетчера от возможных изменений субъектами доступа с целью влияния на процесс его функционирования;
- требование формальной проверки правильности функционирования;
- минимизация используемых диспетчером ресурсов.

В самом общем виде работа средств управления доступом субъектов к объектам основана на проверке сведений, хранимых в базе данных защиты.

Под ***базой данных защиты*** (security database) понимают базу данных, хранящую информацию о правах доступа субъектов системы к объектам и другим субъектам.

Для внесения изменений в базу данных защиты система разграничения доступа должна включать средства для привилегированного пользователя (администратора безопасности) по ведению этой базы. Такие средства управления доступом должны обеспечивать возможность выполнения следующих операций:

- добавления и удаления объектов и субъектов;
- просмотра и изменения соответствующих прав доступа субъектов к объектам.

Форма представления базы данных защиты может быть различной.

Основу базы данных защиты в общем случае составляет матрица доступа или ее представления (см. табл. 3) Каждый элемент этой матрицы представляет собой кортеж, определяющий права доступа (для всех возможных видов доступа) каждого субъекта к каждому объекту или другому субъекту.

Сложность управления доступом (ведения матрицы доступа) в реальных системах связана не только с большой размерностью матрицы (большим числом субъектов и объектов) и высоким динамизмом ее корректировки, но и с необходимостью постоянного отслеживания при таких корректировках большого числа зависимостей между значениями определенных кортежей. Наличие таких зависимостей связано с объективно существующими в предметной области ограничениями и правилами наследования полномочий в иерархии объектов и субъектов. Например, пользователь должен наследовать полномочия группы пользователей, в которую он входит; права доступа некоторого пользователя к каталогам и файлам не должны превышать соответствующие его права по доступу к диску, на котором они размещены и т.п.).

При полномочном управлении доступом (категорирование объектов и субъектов и введение ограничений по доступу установленных категорий субъектов к объектам различных категорий) на матрицу доступа накладываются дополнительные зависимости между значениями прав доступа субъектов.

Существующие ограничения и зависимости между полномочиями существенно усложняют процедуры ведения матриц доступа. Это привело к возникновению большого числа способов неявного задания матрицы (списки доступа, перечисление полномочий, атрибутная схема и т.п.).

Основные критерии оценки эффективности различных способов неявного задания следующие:

- затраты памяти на хранение образа матрицы доступа;
- время на выборку (вычисление) значений полномочий (элементов кортежей);
- удобство ведения матрицы при наличии ограничений и зависимостей между значениями ее кортежей (простота и наглядность, количество требуемых операций при добавлении/удалении субъекта или объекта, назначении/модификации полномочий и т.п.).

Рассмотрим основные способы неявного задания матрицы доступа.

Списки управления доступом к объекту

В данной схеме полномочия доступа к объекту представляются в виде списков (цепочек) кортежей для всех субъектов, имеющих доступ к данному объекту. Это равносильно представлению матрицы по столбцам с исключением кортежей, имеющих все нулевые значения.

Такое представление матрицы доступа получило название "списка управления доступом" (access control list). Этот вид задания матрицы реализован в сетевой ОС Novell NetWare.

Достоинства:

- экономия памяти, так как матрица доступа обычно сильно разрежена;
- удобство получения сведений о субъектах, имеющих какой либо вид доступа к заданному объекту;

Недостатки:

- неудобство отслеживания ограничений и зависимостей по наследованию полномочий субъектов;
- неудобство получения сведений об объектах, к которым имеет какой либо вид доступа данный субъект;
- так как списки управления доступом связаны с объектом, то при удалении субъекта возможно возникновение ситуации, при которой объект может быть доступен несуществующему субъекту.

Списки полномочий субъектов

В данной модели полномочия доступа субъекта представляются в виде списков (цепочек) кортежей для всех объектов, к которым он имеет доступ (любого вида). Это равносильно представлению матрицы по строкам с исключением кортежей, имеющих нулевые значения.

Такое представление матрицы доступа называется "профилем" (profile) субъекта.

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 операций 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.

Достоинства:

- экономия памяти, так как матрица доступа обычно сильно разрежена;
- удобство получения сведений об объектах, к которым имеет какой либо вид доступа данный субъект;

Недостатки:

- неудобство отслеживания ограничений и зависимостей по наследованию полномочий доступа к объектам;
- неудобство получения сведений о субъектах, имеющих какой либо вид доступа к заданному объекту;
- так как списки управления доступом связаны с субъектом, то при удалении объекта возможно возникновение ситуации, при которой субъект может иметь права на доступ к несуществующему объекту.

Атрибутные схемы

Так называемые атрибутные способы задания матрицы доступа основаны на присвоении субъектам и/или объектам определенных меток, содержащих значения атрибутов.

Наиболее известным примером неявного задания матрицы доступа является реализация атрибутной схемы в операционной системе UNIX.

Основными достоинствами этих схем являются:

- экономия памяти, так как элементы матрицы не хранятся, а динамически вычисляются при попытке доступа для конкретной пары субъект-объект на основе их меток или атрибутов;
- удобство корректировки базы данных защиты, то есть модификации меток и атрибутов;
- удобство отслеживания ограничений и зависимостей по наследованию полномочий субъектов, так как они в явном виде не хранятся, а формируются динамически;
- отсутствие потенциальной противоречивости.

Недостатки:

- затраты времени на динамическое вычисление значений элементов матрицы при каждом обращении любого субъекта к любому объекту;
- при атрибутной схеме затруднено задание прав доступа конкретного субъекта к конкретному объекту.

Криптографические методы защиты. Виды средств криптозащиты данных. Достоинства и недостатки. Место и роль средств криптозащиты

Криптографические методы защиты основаны на возможности осуществления некоторой операции преобразования информации, которая может выполняться одним или более пользователем АС, обладающим некоторой секретной частью дополнительной информации, без знания которой с большой вероятностью, невозможно осуществить эту операцию [29].

В классической криптографии используется только одна единица конфиденциальной и обязательно секретной информации - ключ, знание которого позволяет отправителю зашифровать информацию, а получателю - расшифровать ее. Именно эта операция зашифрования/расшифрования с большой вероятностью невыполнима без знания секретного ключа.

В криптографии с открытым ключом имеется два ключа, по крайней мере один из которых нельзя вычислить из другого. Один ключ используется отправителем для зашифрования информации, сохранность которой должна быть обеспечена. Другой ключ используется получателем для обработки полученной информации. Бывают приложения, в которых один ключ должен быть несекретным, а другой - секретным.

Криптографические методы защиты позволяют решать следующие задачи:

- закрытие данных, хранимых в АС или передаваемых по каналам связи;
- контроль целостности и аутентичности данных, передаваемых по каналам связи. Основным достоинством криптографических методов защиты информации является то, что они обеспечивают гарантированную стойкость защиты, которую можно рассчитать и выразить в числовой форме (средним числом операций или количеством времени, необходимого для раскрытия зашифрованной информации или вычисления ключей).

Однако, криптографические методы обладают и существенными недостатками, к числу которых можно отнести следующие:

- низкое быстродействие существующих алгоритмов шифрования (ГОСТ 28147-89);

- трудности с совместным использованием зашифрованной информации;
- высокие требования к сохранности секретного ключа;
- трудности с применением в отсутствии средств защиты от НСД.

Эти недостатки принципиально преодолимы, однако их преодоление может привести к полной неработоспособности системы защиты.

Средства шифрования могут быть реализованы как аппаратно, так и чисто программно. В любом случае они должны быть сертифицированными, то есть должны соответствовать определенным требованиям (стандартам). В противном случае, они не могут гарантировать пользователям необходимую стойкость шифрования.

Использование в системе защиты для различных целей нескольких однотипных алгоритмов шифрования нерационально. Оптимальным вариантом можно считать такую систему, в которой средства криптозащиты являются общесистемными, то есть выступают в качестве расширения функций операционной системы и включают сертифицированные алгоритмы шифрования всех типов (блочные и потоковые, с закрытыми и открытыми ключами).

Прозрачное шифрование всей информации на дисках, что широко рекомендуется рядом разработчиков средств защиты, оправдано лишь в том случае, когда компьютер используется только одним пользователем и объемы дисков невелики. Но на практике даже персональные ЭВМ используются группами из нескольких пользователей. И не только потому, что ПЭВМ на всех не хватает, но и в силу специфики работы защищенных систем. К примеру, автоматизированные рабочие места операторов систем управления используются двумя-четырьмя операторами, работающими посменно, и считать их за одного пользователя нельзя в силу требований разделения ответственности. Очевидно, что в такой ситуации приходится либо отказаться от разделения ответственности и разрешить пользоваться ключом шифра нескольким операторам, либо создавать отдельные закрытые диски для каждого из них и запретить им тем самым обмен закрытой информацией, либо часть информации хранить и передавать в открытом виде, что по сути равносильно отказу от концепции прозрачного шифрования всей информации на дисках.

Кроме того, прозрачное шифрование дисков, требует значительных накладных расходов ресурсов системы (времени и производительности). И не только непосредственно в процессе чтения-записи данных. Дело в том, что

надежное криптографическое закрытие информации предполагает периодическую смену ключей шифрования, а это приводит к необходимости перешифрования всей информации на диске с использованием нового ключа (необходимо всю информацию расшифровать с использованием старого и зашифровать с использованием нового ключа). Это занимает значительное время. Кроме того, при работе в системе с шифрованными дисками задержки возникают не только при обращении к данным, но и при запуске программ, что сильно замедляет работу компьютера.

Поэтому, использовать криптографическую защиту необходимо ограниченно, защищая только ту информацию, которую действительно надо закрыть от несанкционированного доступа.

Целесообразно применение криптографических методов защиты для решения следующих задач :

- для аутентификации пользователей системы (особенно удаленных);
- для закрытия и контроля целостности информации, передаваемой по каналам связи;
- для закрытия конфиденциальной информации в АС (на системном уровне для защиты критичной информации операционной системы и самой системы безопасности, на прикладном уровне - для закрытия секретной и конфиденциальной информации пользователей.).

Управление механизмами защиты

Конкуренция в области разработки средств защиты компьютерных систем неизбежно приводит к унификации перечня общих требований к таким средствам. Одним из пунктов в таком унифицированном списке практически всегда можно встретить требование наличия средств управления всеми имеющимися защитными механизмами. К сожалению, кроме того, что средства управления в системе должны быть, в лучшем случае, для вычислительных сетей, можно встретить лишь уточнение о необходимости обеспечения централизованного удаленного контроля и управления защитными механизмами. Разработчики систем защиты основное внимание уделяют реализации самих защитных механизмов, а не средств управления ими. Такое положение дел свидетельствует о незнании или непонимании и недооценке проектировщиками и разработчиками большого числа психологических и технических препятствий, возникающих при внедрении разработанных систем защиты. Успешно преодолеть эти препятствия можно только, обеспечив необходимую гибкость управления средствами защиты.

Недостаточное внимание к проблемам и пожеланиям заказчиков, к обеспечению удобства работы администраторов безопасности по управле-

нию средствами защиты на всех этапах жизненного цикла компьютерных систем часто является основной причиной отказа от использования конкретных средств защиты.

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

В настоящее время в большинстве случаев установка средств защиты производится на уже реально функционирующие АС заказчика. Защищаемая АС используется для решения важных прикладных задач, часто в непрерывном технологическом цикле, и ее владельцы и пользователи крайне негативно относятся к любому, даже кратковременному, перерыву в ее функционировании для установки и настройки средств защиты или частичной потере работоспособности АС вследствие некорректной работы средств защиты.

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

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

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

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

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

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

Для решения проблем управления средствами защиты в больших сетях в системе необходимо предусмотреть следующие возможности :

- должны поддерживаться возможности управления механизмами защиты как централизованно (удаленно, с рабочего места администратора безопасности сети), так и децентрализовано (непосредственно с конкретной рабочей станции). Причем любые изменения настроек защитных механизмов, произведенные централизованно, должны автоматически распространяться на все рабочие станции, которых они касаются (независимо от состояния рабочей станции на момент внесения изменений в центральную базу данных). Аналогично, часть изменений, произведенных децентрализовано, должна быть автоматически отражена в центральной базе данных защиты и при необходимости также разослана на все другие станции, которых они касаются. Например, при смене своего пароля пользователем, осуществленной на одной из рабочих станций, новое значение пароля этого пользователя должно быть отражено в центральной базе данных защиты сети, а также разослано на все рабочие станции, на которых данному пользователю разрешено работать;
- управление механизмами защиты конкретной станции должно осуществляться независимо от активности данной станции, то есть незави-

симо от того, включена она в данный момент времени и работает ли на ней какой-то пользователь или нет. После включения неактивной станции все изменения настроек, касающиеся ее механизмов защиты, должны быть автоматически перенесены на нее.

- в крупных АС процедура замены версий программ средств защиты (равно как и любых других программ) требует от обслуживающего персонала больших трудозатрат и связана с необходимостью обхода всех рабочих станций для получения к ним непосредственного доступа. Проведение таких замен может быть вызвано как необходимостью устранения обнаруженных ошибок в программах, так и потребностью совершенствования и развития системы (установкой новых улучшенных версий программ);
- для больших АС особую важность приобретает оперативный контроль за состоянием рабочих станций и работой пользователей в сети. Поэтому система защиты в свой состав должна включать подсистему оперативного контроля состояния рабочих станций сети и слежения за работой пользователей.

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

Для облегчения работы администратора с системными журналами в системе должны быть предусмотрены следующие возможности :

- подсистема реализации запросов, позволяющая выбирать из собранных системных журналов данные об определенных событиях (по имени пользователя, дате, времени происшедшего события, категории происшедшего события и т.п.). Естественно такая подсистема должна опираться на системный механизм обеспечения единого времени событий;
- возможность автоматического разбиения и хранения системных журналов по месяцам и дням в пределах заданного количества последних дней. Причем во избежание переполнения дисков по истечении установленного количества дней просроченные журналы, если их не удалил администратор, должны автоматически уничтожаться.
- в системе защиты должны быть предусмотрены механизмы семантического сжатия данных в журналах регистрации, позволяющие укруп-

нять регистрируемые события без существенной потери их информативности. Например, заменять все многократно повторяющиеся в журнале события, связанные с выполнением командного файла autoexec.bat, одним обобщенным. Аналогично можно одним событием заменять многократно повторяющуюся последовательность запуска программ системы MS-Windows и т.п.;

- желательно также иметь в системе средства автоматической подготовки отчетных документов установленной формы о работе станций сети и имевших место нарушениях. Такие средства позволили бы существенно снять рутинную нагрузку с администрации безопасности.

Выводы

В арсенале специалистов по информационной безопасности имеется широкий спектр защитных мер: законодательных, морально-этических, административных (организационных), физических и технических (аппаратурных и программных) средств. Все они обладают своими достоинствами и недостатками, которые необходимо знать и правильно учитывать при создании систем защиты.

При построении конкретных систем компьютерной безопасности необходимо руководствоваться основными принципами организации защиты: системностью, комплексностью, непрерывностью защиты, разумной достаточностью, гибкостью управления и применения, открытостью алгоритмов и механизмов защиты и простотой применения защитных мер и средств, а также придерживаться рекомендаций, полученных на основе опыта предыдущих разработок.

Основными известными универсальными защитными механизмами являются:

- идентификация (именование и опознавание) , аутентификация (подтверждение подлинности) и авторизация субъектов доступа;
- контроль (разграничение) доступа к ресурсам системы;
- регистрация и анализ событий, происходящих в системе;
- криптографическое закрытие, контроль целостности и аутентичности данных, хранимых в АС и передаваемых по каналам связи;
- контроль целостности ресурсов системы.

Эти универсальные механизмы защиты обладают своими достоинствами и недостатками и могут применяться в различных вариациях и совокупностях в конкретных методах и средствах защиты.

Все известные каналы проникновения и утечки информации должны быть перекрыты с учетом анализа риска, вероятностей реализации угроз безопасности в конкретной прикладной системе и обоснованного рационального уровня затрат на защиту.

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

Повышать уровень стойкости системы защиты за счет применения более совершенных физических и технических средств можно только до уровня стойкости персонала из ядра безопасности системы.

На наш взгляд, в ближайшее время успех или неудача масштабного применения систем защиты информации будет зависеть от наличия в них развитых средств управления режимами работы защитными механизмами, и реализации функций, позволяющих существенно упрощать процессы установки, настройки и эксплуатации средств защиты.

4. ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ В АС

Достижение высокого уровня безопасности невозможно без принятия должных организационных мер. С одной стороны, эти меры должны быть направлены на обеспечение правильности функционирования механизмов защиты и выполняться администратором безопасности системы. С другой стороны, руководство организации, эксплуатирующей средства автоматизации, должно регламентировать правила автоматизированной обработки информации, включая и правила ее защиты, а также установить меру ответственности за нарушение этих правил.

Организационная структура, основные функции службы компьютерной безопасности

Для непосредственной организации (построения) и эффективного функционирования системы защиты информации в АС может быть (а при больших объемах защищаемой информации - должна быть) создана специальная штатная служба защиты (служба компьютерной безопасности) [7].

Служба компьютерной безопасности представляет собой штатное или нештатное подразделение, создаваемое для организации квалифицированной разработки системы защиты информации и обеспечения ее функционирования.

Основные функции службы заключаются в следующем [7]:

- формирование требований к системе защиты в процессе создания АС;
- участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;
- планирование, организация и обеспечение функционирования системы защиты информации в процессе функционирования АС;
- распределение между пользователями необходимых реквизитов защиты;
- наблюдение за функционированием системы защиты и ее элементов;
- организация проверок надежности функционирования системы защиты;
- обучение пользователей и персонала АС правилам безопасной обработки информации;
- контроль за соблюдением пользователями и персоналом АС установленных правил обращения с защищаемой информацией в процессе ее автоматизированной обработки;

- принятие мер при попытках НСД к информации и при нарушениях правил функционирования системы защиты.

Организационно-правовой статус службы защиты определяется следующим образом:

- численность службы защиты должна быть достаточной для выполнения всех перечисленных выше функций;
- служба защиты должна подчиняться тому лицу, которое в данном учреждении несет персональную ответственность за соблюдение правил обращения с защищаемой информацией;
- штатный состав службы защиты не должен иметь других обязанностей, связанных с функционированием АС;
- сотрудники службы защиты должны иметь право доступа во все помещения, где установлена аппаратура АС и право прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации;
- руководителю службы защиты должно быть предоставлено право запрещать включение в число действующих новые элементы АС, если они не отвечают требованиям защиты информации;
- службе защиты информации должны обеспечиваться все условия, необходимые для выполнения своих функций.

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

- ***Сотрудник группы безопасности***. В его обязанности входит обеспечение должного контроля за защитой наборов данных и программ, помощь пользователям и организация общей поддержки групп управления защитой и менеджмента в своей зоне ответственности. При децентрализованном управлении каждая подсистема АС имеет своего сотрудника группы безопасности.
- ***Администратор безопасности системы.*** В его обязанности входит ежемесячное опубликование нововведений в области защиты, новых стандартов, а также контроль за выполнением планов непрерывной работы и восстановления (если в этом возникает необходимость) и за хранением резервных копий.
- ***Администратор безопасности данных***. В его обязанности входит реализация и изменение средств защиты данных, контроль за состоя-

нием защиты наборов данных, ужесточение защиты в случае необходимости, а также координирование работы с другими администраторами.

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

Существуют различные варианты детально разработанного штатного расписания такой группы, включающие перечень функциональных обязанностей, необходимых знаний и навыков, распределение времени и усилий. При организации защиты существование такой группы и детально разработанные обязанности ее сотрудников совершенно необходимы [31].

Основные организационные и организационно-технические мероприятия по созданию и поддержанию функционирования комплексной системы защиты

Они включают:

- разовые (однократно проводимые и повторяемые только при полном пересмотре принятых решений) мероприятия;
- мероприятия, проводимые при осуществлении или возникновении определенных изменений в самой защищаемой АС или внешней среде (по необходимости);
- периодически проводимые (через определенное время) мероприятия;
- постоянно (непрерывно или дискретно в случайные моменты времени) проводимые мероприятия.

Разовые мероприятия

К разовым мероприятиям относят:

- общесистемные мероприятия по созданию научно-технических и методологических основ (концепции и других руководящих документов) защиты АС;

- мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов АС (исключение возможности тайного проникновения в помещения, исключение возможности установки прослушивающей аппаратуры и т.п.);
- мероприятия, осуществляемые при проектировании, разработке и вводе в эксплуатацию технических средств и программного обеспечения (проверка и сертификация используемых технических и программных средств, документирование и т.п.);
- проведение спецпроверок всех применяемых в АС средств вычислительной техники и проведения мероприятий по защите информации от утечки по каналам побочных электромагнитных излучений и наводок;
- разработка и утверждение функциональных обязанностей должностных лиц службы компьютерной безопасности;
- внесение необходимых изменений и дополнений во все организационно-распорядительные документы (положения о подразделениях, функциональные обязанности должностных лиц, инструкции пользователей системы и т.п.) по вопросам обеспечения безопасности программно-информационных ресурсов АС и действиям в случае возникновения кризисных ситуаций;
- оформление юридических документов (в форме договоров, приказов и распоряжений руководства организации) по вопросам регламентации отношений с пользователями (клиентами), работающими в автоматизированной системе, между участниками информационного обмена и третьей стороной (арбитражем, третейским судом) о правилах разрешения споров, связанных с применением электронной подписи;
- определение порядка назначения, изменения, утверждения и предоставления конкретным должностным лицам необходимых полномочий по доступу к ресурсам системы;
- мероприятия по созданию системы защиты АС и созданию инфраструктуры;
- мероприятия по разработке правил управления доступом к ресурсам системы (определение перечня задач, решаемых структурными подразделениями организации с использованием АС, а также используемых при их решении режимов обработки и доступа к данным; определение перечня файлов и баз данных, содержащих сведения, составляющие коммерческую и служебную тайну, а также требования к уровням их защищенности от НСД при передаче, хранении и обработке в АС; выявление наиболее вероятных угроз для данной АС, выявле-

ние уязвимых мест процесса обработки информации и каналов доступа к ней; оценку возможного ущерба, вызванного нарушением безопасности информации, разработку адекватных требований по основным направлениям защиты);

- организацию надежного пропускного режима;
- определение порядка учета, выдачи, использования и хранения съемных магнитных носителей информации, содержащих эталонные и резервные копии программ и массивов информации, архивные данные и т.п.;
- организацию учета, хранения, использования и уничтожения документов и носителей с закрытой информацией;
- определение порядка проектирования, разработки, отладки, модификации, приобретения, специсследования, приема в эксплуатацию, хранения и контроля целостности программных продуктов, а также порядок обновления версий используемых и установки новых системных и прикладных программ на рабочих местах защищенной системы (кто обладает правом разрешения таких действий, кто осуществляет, кто контролирует и что при этом они должны делать);
- создание отделов (служб) компьютерной безопасности или, в случае небольших организаций и подразделений, назначение нештатных ответственных, осуществляющих единое руководство, организацию и контроль за соблюдением всеми категориями должностных лиц требований по обеспечению безопасности программно-информационных ресурсов автоматизированной системы обработки информации;
- определение перечня необходимых регулярно проводимых превентивных мер и оперативных действий персонала по обеспечению непрерывной работы и восстановлению вычислительного процесса АС в критических ситуациях, возникающих как следствие НСД, сбоев и отказов СВТ, ошибок в программах и действиях персонала, стихийных бедствий.

Периодически проводимые мероприятия

К периодически проводимым мероприятиям относят:

- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);
- анализ системных журналов, принятие мер по обнаруженным нарушениям правил работы;

- мероприятия по пересмотру правил разграничения доступа пользователей к информации в организации;
- периодически с привлечением сторонних специалистов осуществление анализа состояния и оценки эффективности мер и применяемых средств защиты. На основе полученной в результате такого анализа информации принимать необходимые меры по совершенствованию системы защиты;
- мероприятия по пересмотру состава и построения системы защиты.

Мероприятия, проводимые по необходимости

К мероприятиям, проводимым по необходимости, относят:

- мероприятия, осуществляемые при кадровых изменениях в составе персонала системы;
- мероприятия, осуществляемые при ремонте и модификациях оборудования и программного обеспечения (строгое санкционирование, рассмотрение и утверждение всех изменений, проверка их на удовлетворение требованиям защиты, документальное отражение изменений и т.п.);
- мероприятия по подбору и расстановке кадров (проверка принимаемых на работу, обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, создание условий, при которых персоналу было бы невыгодно нарушать свои обязанности и т.д.).

Постоянно проводимые мероприятия

Постоянно проводимые мероприятия включают:

- мероприятия по обеспечению достаточного уровня физической защиты всех компонентов АС (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности СВТ, носителей информации и т.п.).
- мероприятия по непрерывной поддержке функционирования и управлению используемыми средствами защиты;
- явный и скрытый контроль за работой персонала системы;
- контроль за реализацией выбранных мер защиты в процессе проектирования, разработки, ввода в строй и функционирования АС;

- постоянно (силами отдела (службы) безопасности) и периодически (с привлечением сторонних специалистов) осуществляемый анализ состояния и оценка эффективности мер и применяемых средств защиты.

Перечень основных нормативных и организационно-распорядительных документов, необходимых для организации комплексной системы защиты информации от НСД

Для организации и обеспечения эффективного функционирования комплексной системы компьютерной безопасности должны быть разработаны следующие группы организационно-распорядительных документов:

- документы, определяющие порядок и правила обеспечения безопасности информации при ее обработке в АС (план защиты информации в АС, план обеспечения непрерывной работы и восстановления информации);
- документы, определяющие ответственность взаимодействующих организаций (субъектов) при обмене электронными документами (договор об организации обмена электронными документами).

План защиты информации в АС должен содержать следующие сведения:

- описание защищаемой системы (основные характеристики защищаемого объекта): назначение АС, перечень решаемых АС задач, конфигурация, характеристики и размещение технических средств и программного обеспечения, перечень категорий информации (пакетов, файлов, наборов и баз данных, в которых они содержатся), подлежащих защите в АС и требований по обеспечению доступности, конфиденциальности, целостности этих категорий информации, список пользователей и их полномочий по доступу к ресурсам системы и т.п.;
- цель защиты системы и пути обеспечения безопасности АС и циркулирующей в ней информации;
- перечень значимых угроз безопасности АС, от которых требуется защита и наиболее вероятных путей нанесения ущерба;
- основные требования к организации процесса функционирования АС и мерам обеспечения безопасности обрабатываемой информации ;
- требования к условиям применения и определение зон ответственности установленных в системе технических средств защиты от НСД;

- основные правила, регламентирующие деятельность персонала по вопросам обеспечения безопасности АС (особые обязанности должностных лиц АС).

План обеспечения непрерывной работы и восстановления информации должен отражать следующие вопросы:

- цель обеспечения непрерывности процесса функционирования АС, своевременность восстановления ее работоспособности и чем она достигается;
- перечень и классификация возможных кризисных ситуаций;
- требования, меры и средства обеспечения непрерывной работы и восстановления процесса обработки информации (порядок создания, хранения и использования резервных копий информации и дублирующих ресурсов и т.п.);
- обязанности и порядок действий различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий, минимизации наносимого ущерба и восстановлению нормального процесса функционирования системы.

Договор о порядке организации обмена электронными документами должен включать документы, в которых отражаются следующие вопросы:

- разграничение ответственности субъектов, участвующих в процессах обмена электронными документами;
- определение порядка подготовки, оформления, передачи, приема, проверки подлинности и целостности электронных документов;
- определение порядка генерации, сертификации и распространения ключевой информации (ключей, паролей и т.п.);
- определение порядка разрешения споров в случае возникновения конфликтов.

Выводы

Организационные меры являются той основой, которая объединяет различные меры защиты в единую систему.

Выполнение различных мероприятий по созданию и поддержанию работоспособности системы защиты должно быть возложено на специальную службу - службу компьютерной безопасности.

Обязанности должностных лиц должны быть определены таким образом, чтобы при эффективной реализации ими своих функций, обеспечивалось разделение их полномочий и ответственности.

ЗАКЛЮЧЕНИЕ

Острота проблемы защиты информационных технологий в современных условиях определяется следующими факторами:

- высокими темпами роста парка средств вычислительной техники и связи, расширением областей использования ЭВМ, многообразием и повсеместным распространением информационно-управляющих систем, подлежащих защите;
- вовлечением в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей;
- повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических технологиях;
- отношением к информации, как к товару, переходом к рыночным отношениям, с присущей им конкуренцией и промышленным шпионажем, в области создания и сбыта (предоставления) информационных услуг;
- концентрацией больших объемов информации различного назначения и принадлежности на электронных носителях;
- наличием интенсивного обмена информацией между участниками этого процесса;
- количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам;
- обострением противоречий между объективно существующими потребностями общества в расширении свободного обмена информацией и чрезмерными или наоборот недостаточными ограничениями на ее распространение и использование;
- дифференциацией уровней потерь (ущерба) от уничтожения, фальсификации, разглашения или незаконного тиражирования информации (уязвимости различных затрагиваемых субъектов);
- многообразием видов угроз и возможных каналов несанкционированного доступа к информации;
- ростом числа квалифицированных пользователей вычислительной техники и возможностей по созданию ими программно-математических воздействий на систему;

- развитием рыночных отношений (в области разработки, поставки, обслуживания вычислительной техники, разработки программных средств, в том числе средств защиты).

Естественно, в такой ситуации возникает потребность в защите вычислительных систем и информации от несанкционированного доступа, кражи, уничтожения и других преступных и нежелательных действий.

Наблюдается большая разнородность целей и задач защиты - от обеспечения государственной безопасности до защиты интересов отдельных организаций, предприятий и частных лиц, дифференциация самой информации по степени ее уязвимости.

Все перечисленные факторы имеют самое непосредственное отношение к такой бурно прогрессирующей предметной области как банковское дело. Автоматизированные системы обработки информации в банковской сфере выступают в качестве технической основы для развития и совершенствования существующих банковских технологий и платежных систем в частности. Позволяя ускорить процессы движения финансовых ресурсов, АСОБИ способствуют повышению эффективности функционирования всех финансово-кредитных механизмов государства. От качества платежной системы, в конечном счете, существенно зависит эффективность всей экономики.

В условиях обострения конкурентной борьбы между коммерческими банками за завоевание (сохранение) ведущих позиций и привлечение новых клиентов возможно только при условии предоставления большего количества услуг и сокращения времени обслуживания. Это достижимо лишь при обеспечении необходимого уровня автоматизации всех банковских операций. В то же время применение вычислительной техники не только разрешает возникающие проблемы, но и приводит к появлению новых, нетрадиционных для банка угроз.

Анализ существующего положения показывает, что уровень мероприятий по защите информации в банковской сфере, как правило, отстает от темпов автоматизации.

Сложность определения мер защиты банковских информационных технологий и их реализации состоит в том, что:

- на сегодняшний день не существует единой теории защищенных систем, в достаточной мере универсальной в различных предметных областях (как в государственном, так и в коммерческом секторе);
- производители средств защиты в основном предлагают отдельные компоненты для решения частных задач, оставляя решение вопросов формирования системы защиты и совместимости этих средств своим потребителям;

- для обеспечения надежной защиты необходимо решить целый комплекс технических и организационных проблем с разработкой соответствующей документации.

Руководство и отделы автоматизации банков, действующие в условиях дефицита времени, вынуждены самостоятельно разрабатывать концепцию защиты, методики оценки средств защиты и организационные меры поддержки.

Общеизвестно, что создать абсолютно надежную систему защиты невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту. Поэтому можно говорить только о некотором достаточном уровне безопасности, обеспечении такого уровня защиты, когда стоимость ее преодоления становится больше стоимости получаемой при этом информации (достигаемого эффекта), или когда за время получения информации она обесценивается настолько, что усилия по ее получению теряют смысл.

Что же необходимо защищать и от чего надо защищаться?

Защищать необходимо всех субъектов информационных отношений от возможного материального или морального ущерба, который могут нанести им случайные или преднамеренные воздействия на компьютерную систему и информацию.

Защищаться необходимо от таких нежелательных воздействий, как ошибки в действиях обслуживающего персонала и пользователей системы, ошибки в программном обеспечении, преднамеренные действия злоумышленников, сбои и отказы оборудования, стихийные бедствия и аварии. Естественно на основе разумного анализа риска.

Предотвращать необходимо не только несанкционированный доступ к информации с целью ее раскрытия или нарушения ее целостности, но и попытки проникновения с целью нарушения работоспособности этих систем. Защищать необходимо все компоненты систем: оборудование, программы, данные и персонал.

Все усилия по обеспечению внутренней безопасности систем должны фокусироваться на создании надежных и удобных механизмов принуждения всех ее законных пользователей и обслуживающего персонала к безусловному соблюдению требований политики безопасности, то есть установленной в организации дисциплины прямого или косвенного доступа к ресурсам и информации.

Одним из важнейших аспектов проблемы обеспечения безопасности компьютерных систем является выявление, анализ и классификация возможных путей реализации угроз безопасности, то есть возможных каналов несанкционированного доступа к системе с целью нарушения ее работоспо-

собности или доступа к критической информации, а также оценка реальности реализации угроз безопасности и наносимого при этом ущерба.

Предотвратить внедрение программных закладок можно только путем создания замкнутой программной среды, в которой должна быть исключена возможность использования инструментальных программ, с помощью которых можно было бы осуществить корректировку данных и программ на носителях и в памяти. Не должно быть программирующих пользователей, способных создать свои инструментальные средства (разработка и отладка программ должна производиться на компьютерах, не входящих в состав защищенной системы). Все используемые программы должны проходить предварительную сертификацию на предмет отсутствия в них закладок (с анализом всех исходных текстов, документации и т.д.). Все доработки программ также должны проходить сертификацию на безопасность. Целостность и неискаженность программ должна периодически проверяться путем проверки его характеристик (длины, контрольной суммы). Должен осуществляться постоянный контроль, исключающий внедрение программных закладок и распространение вирусов.

Известно большое число как традиционных, так и специфических для распределенных систем путей проникновения и НСД к информации. Нет никаких гарантий невозможности изобретения принципиально новых путей.

На аппаратно-программном уровне (уровне операционных систем) сложнее всего защититься от целенаправленных действий высококвалифицированных в области вычислительной техники и программирования злоумышленников, но именно к этому надо стремиться.

Как строить систему защиты, какие методы и средства можно при этом использовать?

Все известные меры защиты компьютерных систем подразделяются на: законодательные, морально - этические, административные, физические и технические (аппаратурные и программные). Все они имеют свои достоинства и недостатки.

Наилучшие результаты достигаются при системном подходе к вопросам безопасности компьютерных систем и комплексном использовании различных методов и средств их защиты на всех этапах жизненного цикла систем.

Основными универсальными механизмами противодействия угрозам безопасности, реализуемыми в конкретных средствах защиты, являются:

- идентификация (именование и опознавание), аутентификация (подтверждение подлинности) и авторизация (присвоение полномочий) субъектов;
- контроль (разграничение) доступа к ресурсам системы;
- регистрация и анализ событий, происходящих в системе;

- контроль целостности ресурсов системы.

Система защиты должна строиться эшелонированно в виде концентрических колец безопасности (обороны). Самое внешнее кольцо безопасности обеспечивается морально-этическими и законодательными средствами (неотвратимость возмездия за совершенное деяние). Второе кольцо безопасности представлено физическими и организационными средствами - это внешняя защита системы (защита от стихийных бедствий и внешних посягательств). Внутренняя защита (защита от ошибочных и умышленных действий со стороны персонала и законных пользователей) обеспечивается на уровне аппаратуры и операционной системы и представлена линией обороны, исключающей возможность работы посторонних с системой (механизм идентификации и аутентификации), и кольцами защиты всех ресурсов системы от неавторизованного использования (механизм разграничения доступа в соответствии с полномочиями субъекта). Механизмы регистрации событий и обеспечения целостности повышают надежность защиты, позволяя обнаруживать попытки преодоления других уровней защиты и своевременно предпринимать дополнительные меры, а также исключать возможность потери ценной информации из-за отказов и сбоев аппаратуры (резервирование, механизмы отслеживания транзакций). И, наконец, последнее кольцо безопасности представлено средствами прикладной защиты и криптографии.

Организационные меры должны выступать в качестве обеспечения эффективного применения других методов и средств защиты в части, касающейся регламентации действий людей.

Защиту, основанную на административных мерах, надо везде, где только можно, усиливать соответствующими более надежными современными физическими и техническими средствами.

Опыт создания систем защиты позволяет выделить следующие основные принципы построения систем компьютерной безопасности, которые необходимо учитывать при их проектировании и разработке:

- системность подхода;
- комплексность решений;
- непрерывность защиты;
- разумная достаточность средств защиты;
- простота и открытость используемых механизмов защиты;
- минимум неудобств пользователям и минимум накладных расходов на функционирование механизмов защиты.

К сожалению, как и почти любое достижение человеческого гения, компьютер, решая одни экономические и социальные проблемы, одновременно порождает и другие, порою не менее сложные. Сегодня, когда масштабы вы-

пуска и применения средств вычислительной техники в нашей стране должны резко увеличиться, к решению возможных в будущем проблем надо готовиться загодя, чтобы они не застали врасплох.

ЛИТЕРАТУРА

1. Агеев А.С. Компьютерные вирусы и безопасность информации// Зарубежная радиоэлектроника.1989. N 12.

2. Банковское дело : Справ. пособие/ М.Ю. Бабичев, Ю.А. Бабичева, О.В.Трохова, и др.; Под ред. Ю.А. Бабичевой. М.: Экономика, 1993. 397 с.

3. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. М.:Юридическая литература, 1991. 160 с.

4. Безопасность информационных технологий. Выпуск 1.М.:Госкомитет РФ по высшему образованию, МИФИ. 1994. 100 с.

5. Бияшев О.Г., Диев С.И., Размахнин М.К. Основные направления развития и совершенствования криптографического закрытия информации//Зарубежная радиоэлектроника. 1989. N 12.

6. Гайкович В.Ю., Першин А.Ю. Безопасность электронных банковских систем. М.:Единая Европа, 1994. 363 с.

7. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн.М:Энергоатомиздат, 1994.400 с. и 176 с.

8. Герасименко В.А., Размахнин М.К., Родионов В.В. Технические средства защиты информации//Зарубежная радиоэлектроника. 1989. N 12.

9. Герасименко В.А. Проблемы защиты данных в системах их обработки// Зарубежная радиоэлектроника. 1989. N 12.

10. Голубев В.В., Дубров П.А., Павлов Г.А. Компьютерные преступления и защита информации в вычислительных системах //Вычислительная техника и ее применение. М.:Знание, 1990, N 9, С.3-26.

11. Давыдовский А.И., Максимов В.А. Введение в защиту информации// Интеркомпьютер.1990. N 1. С.17-20.

12. Дейтел Г. Введение в операционные системы: В 2-х т. Т.2. Пер. с англ. М.: Мир, 1987. 398 с.

13. Дружинин Г.В.,Сергеева И.В. Качество информации.М.:Радио и связь, 1990. 172 с.

14. Защита информации в персональных ЭВМ/Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. и др. М.:Радио и связь, МП "Веста", 1992. 192 с.

15. Карасик И. Программные и аппаратные средства защиты информации для персональных компьютеров//Компьютер-пресс.1992. N 3. С.37-46.

16. Касперский Е. "Дыры" в MS DOS и программы защиты информации// Компьютер-пресс. 1991. N 10. С.6-14.

17. Кляйн Д. Как защититься от "взломщика". Обзор методов парольной защиты и набор рекомендаций по ее улучшению //Программирование, 1991, N 3, С.59-63.

18. Моисеенков И.Э. Американская классификация и принципы оценивания безопасности компьютерных систем//Компьютер-пресс. 1992. N2,N 3. С.47-54.

19. Моисеенков И.Э. Основы безопасности компьютерных систем//Компьютерпресс.-1991. N10. С.19-24, N11. С.7-21, N12.

20. Родин Г. Некоторые соображения о защите программ//Компьютерпресс.1991. N 10.- С.15-18.

21. Удалов В.И., Спринцис Я.П. Безопасность в среде взаимодействия открытых систем//Автоматика и вычислительная техника.1990.N3, С.3-11.

22. Хофман Л.Дж. Современные методы защиты информации: Пер. с англ.М.:Сов.радио, 1980, 264 с.

23. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Руководящий документ Гостехкомиссии России, М.:ГТК РФ, 1992. 9 с.

24. Термины и определения в области защиты от НСД к информации. Руководящий документ Гостехкомиссии России, М.:ГТК РФ, 1992. 13с.

25. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России, М.:ГТК РФ, 1992. 25с.

26. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.Руководящий документ Гостехкомиссии России, М.: ГТК РФ, 1992. 39с.

27. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. Руководящий документ Гостехкомиссии России,- М.: ГТК РФ, 1992. 29с.

28. Концепция создания системы платежей крупных сумм. Рабочие материалы //Департамент информатизации ЦБ РФ, 1994.

29. Г.Дж. Симмонс. Защита информации. ТИИЭР, т.76 N5, май 1988г.

30. CSC-STD-003-85, Computer Security Requirements Guidance for Applying the Department of Defense System Evaluation Criteria in Specific Environments.

31. Datapro Reports on Information Security, vol.1-3, 1990-1993.

32. DoD 5200.28-STD. Department of Defence Trusted Computer System Evaluation Criteria (TCSEC) 1985.

33. Evaluation Levels Manual, Department of Trade and Industry, Computer Security Branch, Kingsgate House, 66-74, V22.

34. Gladny H.M.- In: Performance of Computer Installation, Berke, 1978, Proceedings, p.151-200.

35. HighLand H.J. Novell network virus alert., C&S,1990, vol.9 num.7., p.570.

36. ISO/DIS 2382/8. Data processing. - Vocabulary - Part 8 : Control, integrity and security. - ISO, 1985, 35 p.

37. ISO/DIS 7498/2. Information Processing Systems - Open Systems Interconnection Reference Model. Part 2: Security Architecture. ISO, 1989.

38. Linde Richard R. Operating System Penetration, Proceedings 1975 NCC, p.361-368.

39. Linden T.A. (editor) Security Analysis and Enhancements of Computer Operating Systems, Institute for Computer Sciences and Technology of National Bureau of Standarts, Washington, D.C.20234, Report NBSIR 76-1041, April 1976.

40. NCSC-TG-001. A Guide to Understanding Audit in Trusted Systems.

41. NCSC-TG-003. A Guide to Understanding Discretionary Access Control in Trusted Systems.

42. NCSC-TG-005. Version-1 Trusted Network Interpretation of the trusted Computer System Evaluation Criteria.

43. NCSC-TG-006. A Guide to Understanding Configuration Management in Trusted Systems.

44. NCSC-TG-009. Version-1, Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria.

45. NCSC-TG-021. Version-1 Draft Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria.

46. I.M.Olson, M.D.Abrams, Computer Acces Policy Choices, Computer& Security, volume 9(1990), number 8, p.p.699-714.

47. T.A. Parker, Security in Open Systems - A Report on the Standart work of ECMA's TC32/TG9,p 38-50 in Proc. 10th Natl. Computer Security Conf., IEEE, Baltimore, September,1987

48. T.A. Parker, Application Access Control Standarts for Distributed Systems., Computer&Security,volume 9, number 6, p.319-330.

49. Straub D.W., Widom C.S. Deviancy by bit and bytes: computer abusers and control measures//Computer security: A Global Challenge. Netherlands,1984, p.431-441.

50. Yves le Roux, Technical Criteria For Security Evaluation Of Information Technology Products/Information Security Guide, 1990/1991, p.p.59-62.

51. National Bureau of Standards, "Data Encryption Standard", January 1977, NIST NBS-FIPS PUB 46.

52. ANSI/X3/SPARC Study Group on Database Management Systems: Interim report, 1975, p.92-141.

53. Security & Protection, 1978, v.10, N2, p.23-40.

ПРИЛОЖЕНИЕ 1

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В ОБЛАСТИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОБРАБОТКИ ИНФОРМАЦИИ (АС) - организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (наборов, баз) данных на различных носителях, персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей государственных органов, общественных или коммерческих организаций (юридических лиц), отдельных граждан (физических лиц) и иных потребителей информации.

ИНФОРМАЦИЯ В АС - сведения о фактах, событиях, процессах и явлениях в некоторой предметной области, включенные в систему обработки информации, или являющиеся ее результатом в различных формах представления на различных носителях и используемые (необходимые) для оптимизации принимаемых решений в процессе управления объектами данной предметной области.

ОБРАБОТКА ИНФОРМАЦИИ В АС - совокупность операций (сбор, накопление, хранение, преобразование, отображение, выдача и т.п.), осуществляемых над информацией (сведениями, данными) с использованием средств АС.

СУБЪЕКТЫ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ - государство, государственные органы, государственные, общественные или коммерческие организации (объединения) и предприятия (юридические лица), отдельные граждане (физические лица) и иные субъекты, взаимодействующие с целью совместной обработки информации.

По отношению к информации, обрабатываемой в АС различные субъекты - участники информационных отношений могут выступать (возможно одновременно) в качестве:

- источников информации;
- пользователей (потребителей) информации;
- собственников (владельцев, распорядителей) информации;
- физических и юридических лиц, о которых собирается и обрабатывается информация;

- владельцев АС и участников процессов обработки и передачи информации и т.д.

ЖИЗНЕННО ВАЖНЫЕ ИНТЕРЕСЫ - совокупность потребностей, удовлетворение которых необходимо для надежного обеспечения существования и возможности прогрессивного развития субъекта (личности, организации, общества или государства).

ДОСТУПНОСТЬ ИНФОРМАЦИИ - свойство системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ - свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ - субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

Объективные предпосылки подобного ограничения доступности информации заключены в необходимости защиты законных интересов некоторых субъектов информационных отношений.

УЯЗВИМОСТЬ СУБЪЕКТА ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ - потенциальная подверженность субъекта нанесению ущерба его жизненно важным интересам посредством воздействия на критичную для него информацию, ее носители и процессы обработки.

УЯЗВИМОСТЬ ИНФОРМАЦИИ - подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности, или неправомерному ее тиражированию.

УГРОЗА ИНТЕРЕСАМ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ - потенциально возможное событие, действие, процесс или явление, которое посредством воздействия на информацию и другие компоненты АС может привести к нанесению ущерба интересам данных субъектов.

УГРОЗА БЕЗОПАСНОСТИ ИНФОРМАЦИИ - потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию.

БЕЗОПАСНОСТЬ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ -защищенность субъектов информационных отношений от

нанесения им материального, морального или иного ущерба путем воздействия на информацию и/или средства ее обработки и передачи.

БЕЗОПАСНОСТЬ АС (компьютерной системы) - защищенность АС от несанкционированного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, незаконной модификации или разрушения ее компонентов.

БЕЗОПАСНОСТЬ ЛЮБОГО КОМПОНЕНТА (РЕСУРСА) АС складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности.

Конфиденциальность компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

Целостность компонента предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени.

Доступность компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ - защищенность технологического процесса переработки информации.

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ - защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

ДОСТУП К ИНФОРМАЦИИ - ознакомление с информацией (копирование, тиражирование), ее модификация (корректировка) или уничтожение (удаление).

ПРАВИЛА РАЗГРАНИЧЕНИЯ ДОСТУПА - совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе.

РАЗГРАНИЧЕНИЕ ДОСТУПА К РЕСУРСАМ АС - это такой порядок использования ресурсов системы, при котором субъекты получают доступ к объектам в строгом соответствии с установленными правилами.

ОБЪЕКТ - пассивный компонент системы, единица ресурса автоматизированной системы (устройство, диск, каталог, файл и т.п.), доступ к которому регламентируется правилами разграничения доступа.

СУБЪЕКТ - активный компонент системы (пользователь, процесс, программа), действия которого регламентируются правилами разграничения доступа.

АВТОРИЗОВАННЫЙ СУБЪЕКТ ДОСТУПА - субъект, которому предоставлены соответствующие права доступа к объектам системы (полномочия).

ДОСТУП К РЕСУРСУ - получение субъектом доступа возможности манипулировать (использовать, управлять, изменять характеристики и т.п.) данным ресурсом.

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП (НСД) - доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа.

НЕСАНКЦИОНИРОВАННОЕ ДЕЙСТВИЕ - действие субъекта в нарушение установленных в системе правил обработки информации.

НАРУШИТЕЛЬ - это лицо (субъект), которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещенных ему действий с данным ресурсом) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства (чисто агентурные методы получения сведений, технические средства перехвата без модификации компонентов системы, штатные средства и недостатки систем защиты, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ и т.п.).

ЗЛОУМЫШЛЕННИК - нарушитель, действующий умышленно из корыстных побуждений.

СИСТЕМА ЗАЩИТЫ АС (ИНФОРМАЦИИ) - совокупность (комплекс) специальных мер правового (законодательного) и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения безопасности АС (циркулирующей в АС информации).

ЗАЩИТА ИНФОРМАЦИИ - непрерывный процесс построения, поддержки нормального функционирования и совершенствования системы защиты информации.

ЦЕЛЬ ЗАЩИТЫ АС (ИНФОРМАЦИИ) - предотвращение или минимизация наносимого ущерба (прямого или косвенного, материального, морального или иного) субъектам информационных отношений посредством нежелательного воздействия на компоненты АС, а также разглашения (утечки), искажения (модификации), утраты (снижения степени доступности) или незаконного тиражирования информации.

ПРАВОВЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ - действующие в стране законы, указы и другие нормативные акты, регламентирующие пра-

вила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.

МОРАЛЬНО-ЭТИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ - традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

ОРГАНИЗАЦИОННЫЕ (АДМИНИСТРАТИВНЫЕ) МЕРЫ ЗАЩИТЫ - это меры, регламентирующие процессы функционирования системы обработки данных, 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 циркулирующей в ней информации.

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 АС и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.

ТЕХНИЧЕСКИЕ (АППАРАТНО-ПРОГРАММНЫЕ) СРЕДСТВА ЗАЩИТЫ - различные электронные устройства и специальные программы, входящие в состав АС, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

АДМИНИСТРАТОР БЕЗОПАСНОСТИ - лицо или группа лиц, ответственных за обеспечение безопасности системы, за реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющих постоянную организационную поддержку функционирования применяемых физических и технических средств защиты.