9. Лекция: Основные программно-технические меры

Основные понятия программно-технического уровня информационной безопасности

Программно-технические меры, то есть меры, направленные на контроль компьютерных сущностей - оборудования, программ и/или данных, образуют последний и самый важный рубеж информационной безопасности. Напомним, что ущерб наносят в основном действия легальных пользователей, по отношению к которым процедурные регуляторы малоэффективны. Главные враги - некомпетентность и неаккуратность при выполнении служебных обязанностей, и только программно-технические меры способны им противостоять.

Компьютеры помогли автоматизировать многие области человеческой деятельности. Вполне естественным представляется желание возложить на них и обеспечение собственной безопасности. Даже физическую защиту все чаще поручают не охранникам, а интегрированным компьютерным системам, что позволяет одновременно отслеживать перемещения сотрудников и по организации, и по информационному пространству.

Это вторая причина, объясняющая важность программно-технических мер.

Следует, однако, учитывать, что быстрое развитие информационных технологий не только предоставляет обороняющимся новые возможности, но и объективно затрудняет обеспечение надежной защиты, если опираться исключительно на меры программно-технического уровня. Причин тому несколько:

- повышение быстродействия микросхем, развитие архитектур с высокой степенью параллелизма позволяет методом грубой силы преодолевать барьеры (прежде всего криптографические), ранее казавшиеся неприступными;
- развитие сетей и сетевых технологий, увеличение числа связей между информационными системами, рост пропускной способности каналов расширяют круг злоумышленников, имеющих техническую возможность организовывать атаки;
- появление новых *информационных сервисов* ведет и к образованию новых уязвимых мест как "внутри" сервисов, так и на их стыках;
- конкуренция среди производителей программного обеспечения заставляет сокращать сроки разработки, что приводит к снижению качества тестирования и выпуску продуктов с дефектами защиты;
- навязываемая потребителям парадигма постоянного наращивания мощности аппаратного и программного обеспечения не позволяет долго оставаться в рамках надежных, апробированных конфигураций и, кроме того, вступает в конфликт с бюджетными ограничениями, из-за чего снижается доля ассигнований на безопасность.

Перечисленные соображения лишний раз подчеркивают важность комплексного подхода к информационной безопасности, а также необходимость гибкой позиции при выборе и сопровождении программно-технических регуляторов.

Центральным для программно-технического уровня является понятие *сервиса безопасности*.

Следуя объектно-ориентированному подходу, при рассмотрении информационной системы с единичным уровнем детализации мы увидим совокупность предоставляемых ею *информационных сервисов*. Назовем их ***основными***. Чтобы они могли функционировать и обладали требуемыми свойствами, необходимо несколько уровней *дополнительных (вспомогательных) сервисов* - от СУБД и мониторов транзакций до ядра операционной системы и оборудования.

К ***вспомогательным*** относятся сервисы безопасности (мы уже сталкивались с ними при рассмотрении стандартов и спецификаций в области ИБ); среди них нас в

первую очередь будут интересовать универсальные, высокоуровневые, допускающие использование различными *основными* и *вспомогательными сервисами*. Далее мы рассмотрим следующие сервисы:

- *идентификация* и *аутентификация*;
- *управление доступом*;
- *протоколирование* и *аудит*;
- *шифрование*;
- *контроль целостности*;
- *экранирование*;
- *анализ защищенности*;
- обеспечение *отказоустойчивости*;
- обеспечение *безопасного восстановления*;
- *туннелирование*;
- *управление*.

Будут описаны требования к *сервисам безопасности*, их функциональность, возможные методы реализации и место в общей архитектуре.

Если сопоставить приведенный перечень сервисов с классами функциональных требований "Общих критериев", то бросается в глаза их существенное несовпадение. Мы не будем рассматривать вопросы, связанные с *приватностью*, по следующей причине. На наш взгляд, *сервис безопасности*, хотя бы частично, должен находиться в распоряжении того, кого он защищает. В случае же с *приватностью* это не так: критически важные компоненты сосредоточены не на клиентской, а на серверной стороне, так что *приватность* по существу оказывается свойством предлагаемой информационной услуги (в простейшем случае *приватность* достигается путем сохранения конфиденциальности серверной регистрационной информации и защитой от перехвата данных, для чего достаточно перечисленных *сервисов безопасности*).

С другой стороны, наш перечень шире, чем в "Общих критериях", поскольку в него входят *экранирование*, *анализ защищенности* и *туннелирование*. Эти сервисы имеют важное значение сами по себе и, кроме того, могут комбинироваться с другими сервисами для получения таких необходимых *защитных средств*, как, например, виртуальные частные сети.

Совокупность перечисленных выше *сервисов безопасности* мы будем называть полным набором. Считается, что его, в принципе, достаточно для построения надежной защиты на программно-техническом уровне, правда, при соблюдении целого ряда дополнительных условий (отсутствие уязвимых мест, безопасное администрирование и т.д.).

Для проведения классификации *сервисов безопасности* и определения их места в общей архитектуре меры безопасности можно разделить на следующие виды:

- *превентивные*, препятствующие нарушениям ИБ;
- меры *обнаружения нарушений*;
- *локализующие*, сужающие зону воздействия нарушений;
- меры по *выявлению нарушителя*;
- меры восстановления режима безопасности.

Большинство *сервисов безопасности* попадает в число *превентивных*, и это, безусловно, правильно. *Аудит* и *контроль целостности* способны помочь в *обнаружении нарушений*; активный *аудит*, кроме того, позволяет запрограммировать реакцию на нарушение с целью локализации и/или прослеживания. Направленность сервисов *отказоустойчивости* и *безопасного восстановления* очевидна. Наконец, *управление* играет инфраструктурную роль, обслуживая все аспекты ИС.

Особенности современных информационных систем, существенные с точки зрения безопасности

Информационная система типичной современной организации является весьма сложным образованием, построенным в многоуровневой архитектуре клиент/сервер, которое пользуется многочисленными внешними сервисами и, в свою очередь, предоставляет собственные сервисы вовне. Даже сравнительно небольшие магазины, обеспечивающие расчет с покупателями по пластиковым картам (и, конечно, имеющие внешний Web-**сервер**), зависят от своих информационных систем и, в частности, от защищенности всех компонентов систем и коммуникаций между ними.

С точки зрения безопасности наиболее существенными представляются следующие аспекты современных ИС:

- **корпоративная сеть** имеет несколько территориально разнесенных частей (поскольку организация располагается на нескольких производственных площадках), связи между которыми находятся в ведении внешнего поставщика сетевых услуг, выходя за пределы зоны, контролируемой организацией;
- корпоративная сеть имеет одно или несколько подключений к **Internet**;
- на каждой из производственных площадок могут находиться критически важные серверы, в доступе к которым нуждаются сотрудники, работающие на других площадках, мобильные пользователи и, возможно, сотрудники других организаций;
- для доступа пользователей могут применяться не только компьютеры, но и потребительские устройства, использующие, в частности, беспроводную связь;
- в течение одного сеанса работы пользователю приходится обращаться к нескольким *информационным сервисам*, опирающимся на разные аппаратно-программные платформы;
- к **доступности** *информационных сервисов* предъявляются жесткие требования, которые обычно выражаются в необходимости круглосуточного функционирования с максимальным временем простоя порядка нескольких минут;
- информационная система представляет собой сеть с **активными агентами**, то есть в процессе работы программные компоненты, такие как **апплеты** или **сервлеты**, передаются с одной машины на другую и выполняются в целевой среде, поддерживая связь с удаленными компонентами;
- не все пользовательские системы контролируются сетевыми и/или системными администраторами организации;
- программное обеспечение, особенно полученное по сети, не может считаться надежным, в нем могут быть ошибки, создающие проблемы в защите;
- конфигурация информационной системы постоянно изменяется на уровнях административных данных, программ и аппаратуры (меняется состав пользователей, их привилегии и версии программ, появляются новые сервисы, новая аппаратура и т.п.).

Следует учитывать еще по крайней мере два момента. Во-первых, для каждого сервиса основные грани ИБ (доступность, целостность, конфиденциальность) трактуются по-своему. Целостность с точки зрения системы *управления* базами данных и с точки зрения почтового сервера - вещи принципиально разные. Бессмысленно говорить о безопасности локальной или иной сети вообще, если сеть включает в себя разнородные компоненты. Следует *анализировать защищенность* сервисов, функционирующих в сети. Для разных сервисов и защиту строят по-разному. Во-вторых, основная угроза информационной безопасности организаций по-прежнему исходит не от внешних злоумышленников, а от собственных сотрудников.

В силу изложенных причин далее будут рассматриваться распределенные, разнородные, многосервисные, эволюционирующие системы. Соответственно, нас будут интересовать решения, ориентированные на подобные конфигурации.

Архитектурная безопасность

Сервисы безопасности, какими бы мощными они ни были, сами по себе не могут гарантировать надежность программно-технического уровня защиты. Только проверенная архитектура способна сделать эффективным объединение сервисов, обеспечить управляемость информационной системы, ее способность развиваться и противостоять новым угрозам при сохранении таких свойств, как высокая производительность, простота и удобство использования.

Теоретической основой решения проблемы архитектурной безопасности является следующее фундаментальное утверждение, которое мы уже приводили, рассматривая интерпретацию "Оранжевой книги" для сетевых конфигураций.

"Пусть каждый субъект (то есть процесс, действующий от имени какого-либо пользователя) заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента. Далее пусть каждый компонент содержит свой монитор обращений, отслеживающий все локальные попытки доступа, и все мониторы проводят в жизнь согласованную политику безопасности. Пусть, наконец, коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации. Тогда совокупность всех мониторов образует единый монитор обращений для всей сетевой конфигурации."

Обратим внимание на три принципа, содержащиеся в приведенном утверждении:

- необходимость выработки и проведения в жизнь единой политики безопасности;
- необходимость обеспечения конфиденциальности и целостности при сетевых взаимодействиях;
- необходимость формирования составных сервисов по содержательному принципу, чтобы каждый полученный таким образом компонент обладал *полным набором защитных средств* и с внешней точки зрения представлял собой единое целое (не должно быть информационных потоков, идущих к незащищенным сервисам).

Если какой-либо (составной) сервис не обладает *полным набором защитных средств* (состав полного набора описан выше), необходимо привлечение дополнительных сервисов, которые мы будем называть экранирующими. Экранирующие сервисы устанавливаются на путях доступа к недостаточно защищенным элементам; в принципе, один такой сервис может *экранировать* (защищать) сколь угодно большое число элементов.

С практической точки зрения наиболее важными являются следующие принципы архитектурной безопасности:

- **непрерывность защиты** в пространстве и времени, невозможность миновать защитные средства;
- следование признанным стандартам, использование апробированных решений;
- иерархическая организация ИС с небольшим числом сущностей на каждом уровне;
- усиление самого **слабого звена;**
- невозможность перехода в **небезопасное состояние;**
- минимизация привилегий;
- разделение обязанностей;
- **эшелонированность обороны;**
- разнообразие защитных средств;
- простота и управляемость информационной системы.

Поясним смысл перечисленных принципов.

Если у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, он, разумеется, так и сделает. Определенные выше экранирующие сервисы должны исключить подобную возможность.

Следование признанным стандартам и использование апробированных решений повышает надежность ИС и уменьшает вероятность попадания в тупиковую ситуацию, когда обеспечение безопасности потребует непомерно больших затрат и принципиальных модификаций.

Иерархическая организация ИС с небольшим числом сущностей на каждом уровне необходима по технологическим соображениям. При нарушении данного принципа система станет неуправляемой и, следовательно, обеспечить ее безопасность будет невозможно.

Надежность любой обороны определяется самым слабым звеном. Злоумышленник не будет бороться против силы, он предпочтет легкую победу над слабостью. (Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.)

Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если в крепости механизм подъемного моста ломается, мост оставляют поднятым, препятствуя проходу неприятеля.

Применительно к программно-техническому уровню принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей. Этот принцип позволяет уменьшить ущерб от случайных или умышленных некорректных действий пользователей и администраторов.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, чтобы один человек не мог нарушить критически важный для организации процесс или создать брешь в защите по заказу злоумышленников. В частности, соблюдение данного принципа особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за *идентификацией* и *аутентификацией* - *управление доступом* и, как последний рубеж, - *протоколирование* и *аудит*. Эшелонированная оборона способна, по крайней мере, задержать злоумышленника, а благодаря наличию такого рубежа, как *протоколирование* и *аудит*, его действия не останутся незамеченными. Принцип разнообразия защитных средств предполагает создание различных по своему характеру оборонительных рубежей, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками.

Очень важен принцип простоты и управляемости информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации различных компонентов и осуществлять централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (например, таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и плохо управляемой.

Для обеспечения высокой доступности (непрерывности функционирования) необходимо соблюдать следующие принципы архитектурной безопасности:

- внесение в конфигурацию той или иной формы **избыточности** (резервное оборудование, запасные каналы связи и т.п.);
- наличие средств обнаружения нештатных ситуаций;
- наличие средств **реконфигурирования** для восстановления, **изоляции** и/или замены компонентов, отказавших или подвергшихся атаке на доступность;
- рассредоточенность сетевого *управления*, отсутствие **единой точки отказа;**
- выделение подсетей и изоляция групп пользователей друг от друга. Данная мера, являющаяся обобщением разделения процессов на уровне операционной системы, ограничивает зону поражения при возможных нарушениях информационной безопасности.

Еще один важный архитектурный принцип - минимизация объема защитных средств, выносимых на клиентские системы. Причин тому несколько:

- для доступа в корпоративную сеть могут использоваться **потребительские устройства** с ограниченной функциональностью;
- конфигурацию клиентских систем трудно или невозможно контролировать.

К необходимому минимуму следует отнести реализацию *сервисов безопасности* на сетевом и транспортном уровнях и поддержку механизмов *аутентификации*, устойчивых к сетевым угрозам.