15. Лекция: Заключение

Что такое информационная безопасность. Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности

Цель мероприятий в области **информационной безопасности** - защитить **интересы субъектов информационных отношений**. *Интересы* эти многообразны, но все они концентрируются вокруг трех основных аспектов:

- **доступность**;
- **целостность**;
- **конфиденциальность**.

Первый шаг при построении системы **ИБ** организации - ранжирование и детализация этих аспектов.

Важность проблематики *ИБ* объясняется двумя основными причинами:

- ценностью накопленных информационных ресурсов;
- критической зависимостью от информационных технологий.

Разрушение *важной* информации, кража *конфиденциальных* данных, перерыв в работе вследствие отказа - все это выливается в крупные материальные потери, наносит **ущерб** репутации организации. Проблемы с системами управления или медицинскими системами угрожают здоровью и жизни людей.

Современные информационные системы *сложны* и, значит, опасны уже сами по себе, даже без учета активности злоумышленников. Постоянно обнаруживаются новые **уязвимые места** в программном обеспечении. Приходится принимать во внимание чрезвычайно широкий спектр аппаратного и программного обеспечения, многочисленные связи между компонентами.

Меняются принципы построения корпоративных ИС. Используются многочисленные внешние информационные сервисы; предоставляются вовне собственные; получило широкое распространение явление, обозначаемое исконно русским словом "аутсорсинг", когда часть функций корпоративной ИС передается внешним организациям. Развивается программирование с **активными агентами**.

Подтверждением **сложности** проблематики *ИБ* является параллельный (и довольно быстрый) **рост затрат** на защитные мероприятия и количества **нарушений** *ИБ* в сочетании с *ростом* среднего *ущерба* от каждого *нарушения*. (Последнее обстоятельство - еще один довод в пользу *важности ИБ*.)

Успех в области *информационной безопасности* может принести только комплексный подход, сочетающий меры четырех **уровней**:

- **законодательного**;
- **административного**;
- **процедурного**;
- **программно-технического**.

Проблема *ИБ* - не только (и не столько) техническая; без законодательной базы, без постоянного внимания руководства организации и выделения необходимых ресурсов, без мер управления персоналом и физической защиты решить ее невозможно. Комплексность также усложняет проблематику *ИБ*; требуется взаимодействие специалистов из разных областей.

В качестве основного инструмента борьбы со *сложностью* предлагается **объектно-ориентированный подход**. **Инкапсуляция, наследование, полиморфизм**, выделение **граней** объектов, варьирование **уровня детализации** - все это универсальные понятия, знание которых необходимо всем специалистам по *информационной безопасности*.

Законодательный, административный и процедурный уровни

Законодательный уровень является *важнейшим* для обеспечения *информационной безопасности*. Необходимо всячески подчеркивать *важность* проблемы *ИБ*;

сконцентрировать ресурсы на *важнейших* направлениях исследований; скоординировать образовательную деятельность; создать и поддерживать негативное отношение к нарушителям *ИБ* - все это функции *законодательного уровня*.

На *законодательном уровне* особого внимания заслуживают **правовые акты** и **стандарты**.

Российские правовые акты в большинстве своем имеют ограничительную направленность. Сами по себе **лицензирование** и **сертификация** не обеспечивают безопасности. К тому же в законах не предусмотрена ответственность государственных органов за *нарушения ИБ*. Реальность такова, что в России в деле обеспечения *ИБ* на помощь государства рассчитывать не приходится.

На этом фоне поучительным является знакомство с законодательством США в области *ИБ*, которое гораздо обширнее и многограннее российского.

Среди стандартов выделяются **"Оранжевая книга"**, рекомендации **X.800** и "Критерии оценки безопасности информационных технологий".

"Оранжевая книга" заложила понятийный базис; в ней определяются *важнейшие* **сервисы безопасности** и предлагается метод **классификации** информационных систем по требованиям безопасности.

Рекомендации X.800 весьма глубоко трактуют вопросы защиты **сетевых конфигураций** и предлагают развитый набор сервисов и **механизмов безопасности**.

Международный стандарт ISO 15408, известный как **"Общие критерии"**, реализует более современный подход, в нем зафиксирован чрезвычайно широкий спектр сервисов безопасности (представленных как **функциональные требования**). Его принятие в качестве национального стандарта *важно* не только из абстрактных соображений интеграции в мировое сообщество; оно, как можно надеяться, облегчит жизнь владельцам информационных систем, существенно расширив спектр *доступных* сертифицированных решений.

Главная задача мер *административного уровня* - сформировать программу работ в области *информационной безопасности* и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является **политика безопасности**, отражающая подход организации к защите своих информационных активов.

Разработка политики и **программы безопасности** начинается с **анализа рисков**, первым этапом которого, в свою очередь, является ознакомление с наиболее распространенными **угрозами**.

Главные угрозы - внутренняя *сложность* ИС, непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

На втором месте по размеру *ущерба* стоят кражи и подлоги.

Реальную опасность представляют пожары и другие аварии поддерживающей инфраструктуры.

В общем числе *нарушений* растет доля внешних атак, но основной *ущерб* по-прежнему наносят "свои".

Для подавляющего большинства организаций достаточно общего знакомства с рисками; ориентация на типовые, апробированные решения позволит обеспечить **базовый уровень безопасности** при минимальных интеллектуальных и разумных материальных *затратах*.

Существенную помощь в разработке политики безопасности может оказать британский стандарт BS 7799:1995, предлагающий типовой каркас.

Разработка программы и политики безопасности может служить примером использования понятия *уровня детализации*. Они должны подразделяться на несколько уровней, трактующих вопросы разной степени специфичности. *Важным* элементом программы является разработка и поддержание в актуальном состоянии карты ИС.

Необходимым условием для построения надежной, экономичной защиты является рассмотрение **жизненного цикла** ИС и синхронизация с ним мер безопасности. Выделяют следующие этапы жизненного цикла:

- инициация;
- закупка;
- установка;
- эксплуатация;
- выведение из эксплуатации.

Безопасность невозможно добавить к системе; ее нужно закладывать с самого начала и поддерживать до конца.

Меры *процедурного уровня* ориентированы на людей (а не на технические средства) и подразделяются на следующие виды:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на *нарушения* режима безопасности;
- планирование восстановительных работ.

На этом уровне применимы *важные* принципы безопасности:

- непрерывность защиты в пространстве и времени;
- разделение обязанностей;
- минимизация привилегий.

Здесь также применимы объектный подход и понятие жизненного цикла. Первый позволяет разделить контролируемые сущности (территорию, аппаратуру и т.д.) на относительно независимые подобъекты, рассматривая их с разной степенью детализации и контролируя связи между ними.

Понятие жизненного цикла полезно применять не только к информационным системам, но и к сотрудникам. На этапе инициации должно быть разработано описание должности с требованиями к квалификации и выделяемыми компьютерными привилегиями; на этапе установки необходимо провести обучение, в том числе по вопросам безопасности; на этапе выведения из эксплуатации следует действовать аккуратно, не допуская нанесения *ущерба* обиженными сотрудниками.

Информационная безопасность во многом зависит от аккуратного ведения текущей работы, которая включает:

- поддержку пользователей;
- поддержку программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Элементом повседневной деятельности является отслеживание информации в области *ИБ*; как минимум, администратор безопасности должен подписаться на список рассылки по новым пробелам в защите (и своевременно знакомиться с поступающими сообщениями).

Нужно, однако, заранее готовиться к событиям неординарным, то есть к *нарушениям ИБ*. Заранее продуманная реакция на *нарушения* режима безопасности преследует три главные цели:

- локализация инцидента и уменьшение наносимого вреда;
- выявление нарушителя;
- предупреждение повторных *нарушений*.

Выявление нарушителя - процесс *сложный*, но первый и третий пункты можно и нужно тщательно продумать и отработать.

В случае серьезных аварий необходимо проведение восстановительных работ. Процесс планирования таких работ можно разделить на следующие этапы:

- выявление критически *важных* функций организации, установление приоритетов;
- идентификация ресурсов, необходимых для выполнения критически *важных* функций;
- определение перечня возможных аварий;
- разработка стратегии восстановительных работ;
- подготовка реализации выбранной стратегии;
- проверка стратегии.

Программно-технические меры

Программно-технические меры, то есть меры, направленные на контроль компьютерных сущностей - оборудования, программ и/или данных, образуют последний и самый *важный* рубеж *информационной безопасности*.

На этом рубеже становятся очевидными не только позитивные, но и негативные последствия быстрого прогресса информационных технологий. Во-первых, дополнительные возможности появляются не только у специалистов по *ИБ*, но и у злоумышленников. Во-вторых, информационные системы все время модернизируются, перестраиваются, к ним добавляются недостаточно проверенные компоненты (в первую очередь программные), что затрудняет соблюдение режима безопасности.

Сложность современных корпоративных ИС, многочисленность и разнообразие угроз их безопасности можно наглядно представить, ознакомившись с информационной системой Верховного суда Российской Федерации.

Меры безопасности целесообразно разделить на следующие виды:

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

В продуманной **архитектуре безопасности** все они должны присутствовать.

С практической точки зрения *важными* также 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.

Центральным для *программно-технического уровня* является понятие сервиса безопасности. В число таких сервисов входят:

- **идентификация** и **аутентификация**;
- **управление доступом**;
- **протоколирование** и **аудит**;
- **шифрование**;
- **контроль целостности**;

- **экранирование**;
- **анализ защищенности**;
- обеспечение **отказоустойчивости**;
- обеспечение **безопасного восстановления**;
- **туннелирование**;
- **управление**.

Эти сервисы должны функционировать в открытой сетевой среде с разнородными компонентами, то есть быть устойчивыми к соответствующим угрозам, а их применение должно быть удобным для пользователей и администраторов. Например, современные средства идентификации/аутентификации должны быть устойчивыми к пассивному и активному прослушиванию сети и поддерживать концепцию единого входа в сеть.

Выделим *важнейшие* моменты для каждого из перечисленных сервисов безопасности:

1. Предпочтительными являются **криптографические методы** аутентификации, реализуемые программным или аппаратно-программным способом. Парольная защита стала анахронизмом, биометрические методы нуждаются в дальнейшей проверке в сетевой среде.
2. В условиях, когда понятие доверенного программного обеспечения уходит в прошлое, становится анахронизмом и самая распространенная - произвольная (дискреционная) - модель управления доступом. В ее терминах невозможно даже объяснить, что такое "троянская" программа. В идеале при **разграничении доступа** должна учитываться семантика операций, но пока для этого есть только теоретическая база. Еще один *важный* момент - простота администрирования в условиях большого числа пользователей и ресурсов и непрерывных изменений конфигурации. Здесь может помочь ролевое управление.

Протоколирование и аудит должны быть всепроникающими и многоуровневыми, с фильтрацией данных при переходе на более высокий уровень. Это необходимое условие управляемости. Желательно применение средств **активного аудита**, однако нужно осознавать ограниченность их возможностей и рассматривать эти средства как один из рубежей эшелонированной обороны, причем не самый надежный. Следует конфигурировать их таким образом, чтобы минимизировать число ложных тревог и не совершать опасных действий при автоматическом реагировании.

Все, что связано с криптографией, *сложно* не столько с технической, сколько с юридической точки зрения; для шифрования это верно вдвойне. Данный сервис является инфраструктурным, его реализации должны присутствовать на всех аппаратно-программных платформах и удовлетворять жестким требованиям не только к безопасности, но и к производительности. Пока же единственным *доступным* выходом является применение свободно распространяемого ПО.

Надежный контроль *целостности* также базируется на криптографических методах с аналогичными проблемами и методами их решения. Возможно, принятие Закона об **электронной цифровой подписи** изменит ситуацию к лучшему, будет расширен спектр реализаций. К счастью, к статической *целостности* есть и некриптографические подходы, основанные на использовании запоминающих устройств, данные на которых *доступны* только для чтения. Если в системе разделить статическую и динамическую составляющие и поместить первую в ПЗУ или на компакт-диск, можно в корне пресечь угрозы *целостности*. Разумно, например, записывать регистрационную информацию на устройства с однократной записью; тогда злоумышленник не сможет "замести следы".

Экранирование - идейно очень богатый сервис безопасности. Его реализации - это не только межсетевые экраны, но и ограничивающие интерфейсы, и виртуальные локальные сети. Экран *инкапсулирует* защищаемый объект и контролирует его внешнее представление. Современные межсетевые экраны достигли очень высокого уровня защищенности, удобства использования и администрирования; в сетевой среде они

являются первым и весьма мощным рубежом обороны. Целесообразно применение всех видов МЭ - от персонального до внешнего корпоративного, а контролю подлежат действия как внешних, так и внутренних пользователей.

Анализ защищенности - это инструмент поддержки безопасности жизненного цикла. С активным аудитом его роднит эвристичность, необходимость практически непрерывного обновления базы знаний и роль не самого надежного, но необходимого защитного рубежа, на котором можно расположить свободно распространяемый продукт.

Обеспечение отказоустойчивости и безопасного восстановления - аспекты высокой *доступности*. При их реализации на первый план выходят архитектурные вопросы, в первую очередь - внесение в конфигурацию (как аппаратную, так и программную) определенной избыточности, с учетом возможных угроз и соответствующих зон поражения. Безопасное восстановление - действительно последний рубеж, требующий особого внимания, тщательности при проектировании, реализации и сопровождении.

Туннелирование - скромный, но необходимый элемент в списке сервисов безопасности. Он *важен* не столько сам по себе, сколько в комбинации с шифрованием и экранированием для реализации виртуальных частных сетей.

Управление - это инфраструктурный сервис. Безопасная система должна быть управляемой. Всегда должна быть возможность узнать, что на самом деле происходит в ИС (а в идеале - и получить прогноз развития ситуации). Возможно, наиболее практичным решением для большинства организаций является использование какого-либо свободно распространяемого каркаса с постепенным "навешиванием" на него собственных функций.

Миссия обеспечения *информационной безопасности* трудна, во многих случаях невыполнима, но всегда благородна.