Лекция 13
Информационная безопасность.
Базовые понятия и введение в проблематику

В представлении большинства любителей компьютерных сетей, значительная часть которых к тому же считает себя их знатоками, их *представление о проблематике информационной безопасности компьютерных сетей сводится к представлению о сетевых атаках и сетевых вирусах*. Между тем проблематика компьютерной безопасности компьютерных систем и сетей гораздо шире. В настоящей лекции мы попытаемся дать по возможности широкое представление об этой проблематике, после чего (в следующих лекциях) остановимся на непосредственных и программно-техническим угрозах, представителями которых являются как сетевые атаки, так и вирусы, а затем рассмотрим основные методы и средства борьбы с такими угрозами.

13.1 Определение и основные свойства защищённых компьютерных систем и сетей

Прежде, чем перейти к сути обсуждаемых в настоящем пункте вопросов, отметим, что в рамках настоящего подраздела термины “информационная безопасность” (ИБ) и “защищенность” являются эквивалентными (и то и другое по-английски звучит как “security”). Просто при каждом конкретном использовании одного из этих терминов предпочтение отдаётся тому, который является более благозвучным и/или лаконичным в контексте этого конкретно использования. При этом зачастую предпочтение будет отдаваться термину “защищённость”, поскольку он, на наш взгляд, более адекватно отражает проблему и, в отличие от термина “информационная безопасность” никогда не может быть проинтерпретирован, например, как “представляющий угрозу некоторым внешним объектам”. А такое толкование термина в настоящих лекциях не применяется.

В качестве класса объектов защиты (обеспечения ИБ) нами рассматривается компьютерная система или сеть (КСС). В этот класс объектов входят и одиночный компьютер, подключенный к интернету (или к менее глобальной сети), и подсеть компьютеров, задействованных в работе некоторого распределённого приложения, и корпоративная сеть некоторой организации, и другие виды подсетей, интуитивно ассоциирующихся с термином КСС.

Вкратце рассмотрим ***состав основных компонентов КСС***. В их число входят не только очевидные *компьютеры* (с их аппаратурой, программным

обеспечением, операционными и файловыми системами и пр.), *коммуникационные устройства и каналы связи*. На каждом из компьютеров могут использоваться и используются *внешние носители информации*, к которым относятся не только съёмные носители информации, такие, например, как CD и разнообразные USB-накопители, но и распечатки файлов, изображения на экране монитора, клавиатура (с возможным непредусмотренным наблюдением за процессом нажимания клавиш) и некоторые другие компоненты. После этого перечисления отметим, что нарушение ИБ для любого из этих компонентов КСС может повлечь масштабное нарушение ИБ для всей КСС. Так, если в результате скрытой установки в помещении с одним из компьютеров КСС камеры наблюдения за экраном монитора и клавиатурой будет перехвачен пароль какого-либо из привилегированных пользователей, пострадает ИБ всей КСС. Ситуация не изменится, если такой пароль будет подсмотрен через окно (современная оптика имеет хорошую разрешающую способность). О возможности выноса информации на очень компактных USB-носителях можно было бы и не напоминать . . .

Из рассмотренного следует, что проблема обеспечения ИБ КСС значительно шире, чем кажется, и не сводится к защите от атак и вирусов. Возможные виды угроз ИБ и меры по предотвращению этих угроз рассматриваются нами далее.

Перейдём к определению защищённой КОС. Существуют различные определения защищённой системы. Мы приведём то из них, которое одновременно является и максимально общим и, с другой стороны, очень конкретным.

Определение: Защищенной называется такая КСС, которая:

1) всегда делает то, что она должна делать и

2) никогда не делает того, чего она делать не должна

И действительно, если КСС хотя бы единожды не выполнит в нужный момент требуемую в этот момент функцию, куда же делась защищённость КСС от разрушения её функционала. А если вдруг в один прекрасный момент КСС сделает то, что от неё не требовалось (например, передаст конфиденциальный файл кому-то неизвестному администраторам КСС), то где же находится защищённость КСС.

Рассмотрим основные свойства КСС как объекта защиты. *Три первых из этих свойств упоминаются практически при любом рассмотрении защищённой компьютерной сети или системы*. Но *остальные также являются очень важными*. Перечислим эти свойства:

- ***Конфиденциальность*** (privacy – личная собственность) – защищенность информации, хранящейся в КСС или передаваемой по её каналам связи от несанкционированного доступа к содержанию этой информации.
- ***Целостность*** (integrity) - сохранность данных (например, данных банковского счёта клиента банковской КСС), их защищенность от несанкционированного изменения и/или разрушения.
- ***Доступность*** (availability) – возможность оперативного (в течение короткого критического интервала времени) доступа к требуемой информации. Эта возможность крайне важна для систем реального времени и банковских систем (с б'ольшим, но достаточно коротким критическим интервалом).
- ***Изоляция*** (isolation) – компоненты КСС должны быть по возможности максимально изолированы друг от друга и от внешней среды. Взаимодействие компонентов КСС друг с другом и с "разрешёнными" внешними системами должно выполняться лишь на основе предназначенных для этого интерфейсов. *Компоненты КСС должны рассматривать друг друга и к внешние системы как возможную угрозу своей ИБ и обязательно анализировать правильность переданных параметров*. За счет изоляции затрудняется (в идеале - делается невозможным) распространение нарушения ИБ, произошедшее для одного из компонентов КСС на всю КСС.
- ***Предсказуемость*** (predictability) – идентичность поведения КСС в идентичных ситуациях. Примером систем, не удовлетворяющим этому требованию, являются системы с интерфейсом рабочего стола (Desktop). После того, как на компьютере с таким интерфейсом "поработает" несколько минут злонамеренный или просто чрезмерно активный сторонний пользователь, законный пользователь в нужный момент времени может вдруг не найти пиктограммы срочно требуемого ему приложения. В результате будет не выполнено свойство доступности.
- ***Возможность аудита*** - (auditability) – возможность эффективного анализа (как правило - с использование специальных средств) состояния КСС с

целью выявления попыток (в лучшем случае) или состоявшихся фактов (в худшем случае) нарушения ИБ. Кроме обнаружения указанных фактов средства аудита должны также позволять определить: как произошло нарушение ИБ и что нужно сделать для восстановления нормального состояния КСС. Так, например, известные средства аудита уровня С2, достаточные для банковских систем, обеспечивают возможность для каждого поля каждой записи БД отслеживать информацию о том, когда (момент времени) было выполнено последнее изменение значения этого поля, от имени какого из пользователей это было сделано и каким было значение поля до момента его последнего изменения.

Все рассмотренные свойства защищенной КСС являются очень важными и постоянное выполнение этих свойств, конечно же, является задачей администратора КСС. Однако *он обеспечивает выполнение этих свойств мерами, предпринимаемыми им в соответствии с принятой политикой ИБ (см. далее), при реакции на угрозы ИБ*, рассматриваемые в ниже.

13.2. Основные угрозы ИБ

Начнём с определения: ***угроза ИБ*** - это потенциально возможное событие или явление, в результате реализации которого ИБ КСС может быть нарушена.

Рассмотрим основные типы угроз ИБ КСС начиная с самых разрушительных, но не строго упорядочивая список угроз в порядке уменьшения степени их разрушительности, ибо оценка степени разрушительности той или иной угрозы может существенно зависеть от масштабов и иных особенностей КСС. В число основных типов угроз ИБ входят следующие.

- ***Аварии и стихийные бедствия***. К авариям относятся, например, пожары, прорывы системы отопления, взрывы некоторых технических объектов (например, Чернобыльской АЭС) и прочие разрушения техногенного характера. К числу стихийных бедствий относятся удары молний, землетрясения, наводнения, цунами, падение метеоритов и иные разрушительные явления природы. Обычно стихийные бедствия являются источниками различных аварий. Реализации подобных угроз может приводить к полному разрушению КСС (с автоматической утратой ею всех свойств защищённой КСС). Методы предотвращения аварий и некоторых стихийных бедствий (например – ударов молний) являются предметом,

далёким от компьютерных сетей, но специалисту по ИБ надо хотя бы знать о фактах существования конкретных методов (например, об установке молниеотводов для предотвращения ударов молний), специалист по ИБ должен также понимать, что для компенсации потерь случае реализации различных угроз можно *заключить соответствующий страховой договор*.

- Ликвидация последствий рассмотренных явлений в смысле оперативного восстановления работоспособности и функционального состояния и информационного наполнения КСС может быть выполнена методами резервирования каналов связи, оборудования, систем его программного обеспечения и информационного наполнения. При этом ликвидация последствий масштабных разрушительных явлений возможна лишь в том случае, если резервные “копии” КСС хранятся на достаточном удалении от основной КСС и не пострадали в результате того же разрушительного явления.
- ***Диверсии*** по характеру возникающих разрушительных воздействий и мер, принимаемых для обеспечения возможности оперативного восстановления работоспособности КСС, мало чем отличаются от аварий и стихийных бедствий. Разве что договоры страхования на случай диверсии заключаются в исключительно редких случаях. Но, очевидно, что в случае диверсии обязательно следует обратиться в следственные органы и, после возможного успешного расследования - в судебные органы.
- ***Сбои и отказы в работе оборудования и программного обеспечения*** КСС, собственных и арендуемых каналов передачи данных, каналов доступа к интернету и пр. Для обеспечения возможности оперативного восстановления работы КСС необходимо предусмотреть резервирование оборудования, каналов передачи данных и доступа к интернету, источников электропитания, создание резервных копий данных и пр. и пр. При заключении договоров на аренду каналов передачи данных необходимо оговорить в тексте договора условия наступления и характер ответственности арендодателя за отказы в работе предоставляемых ими услуг, чтобы в случае возникновения таких условий потребовать добровольного или принудительного (по решению судебных органов) возмещения убытков в соответствии с условиями договора.

- ***Ненадёжный персонал***. Два основных вида ненадёжности персонала - это подкупность и халатность. Для уменьшения вероятности подкупа персонала, совершаемого с целью оказания этим персоналом того или иного содействия сторонним лицам или организациям можно рекомендовать достойно оплачивать труд этого персонала (на основе критериев рынка труда соответствующего персонала). Другим рекомендуемым действием является использование принципа “двух ключей от ядерного чемоданчика” - для совершения особо критичных действий в системе (таких, например, как банковских переводов особо крупных сумм) можно требовать авторизации (подтверждения паролями) от нескольких человек. Одновременный подкуп нескольких сотрудников имеет существенно меньшую, чем для одного сотрудника, вероятность осуществления.

  Основным способом борьбы с халатностью сотрудников является разработка их должностных инструкций, строго определяющих права, обязанности и меры ответственности вплоть до уголовных (рассматриваются далее) как *за совершение неправомерных действий*, так и *за невыполнение обязанностей*. И с этими инструкциями сотрудники должны ознакомиться “под подпись”.
- ***Применение злоумышленником технических средств нарушения ИБ***. Основными видами таких средств являются средства прослушивания каналов передачи данных (например, путём:

  - прослушивания электромагнитных полей, возникающих в каналах передачи данных, модулирующих эти данные изменением электрического сигнала),

  - разнообразные средства визуального наблюдения за экранами мониторов и клавиатурами компьютеров,

  - средства аудио прослушивания разговоров в ключевых помещениях КСС (включая столь изощрённые средства, как, например аудио прослушивание путём восстановления речи по колебаниям направления лазерного луча, отражаемого от стеклянных окон помещения).
- Основными методами борьбы с этой угрозой является применение различных мер организационного и технического характера.

- ***Непосредственный доступ злоумышленника к компонентам КСС***. Возможные виды такого доступа включают доступ к терминалу (пусть даже кратковременный, опасность этого рассматривается нами далее), доступ к съемным носителям информации (компактные носители легко вынести из помещения), выброшенным “бракованным” распечаткам и т.д. Для того, чтобы исключить возможность таких видов доступа, в должностные инструкции персонала необходимо включить предписания и запреты, исключающие возможность указанных событий. Кроме того, должны быть обеспечены все необходимые для выполнения таких предписаний средства. Например, в помещениях должны быть установлены сейфы для хранения носителей информации и устройства для измельчения ненужных распечаток.
- ***Использование программно-технических методов нарушения ИБ***. Наконец то мы дошли и до локальных и сетевых атак, вирусов, троянов и сетевых червей, к которым следует присовокупить и опасные действия за привилегированным терминалом не имеющих привилегий лиц, получивших хотя крайне кратковременный (до ~ 30 сек.) доступ к такому терминалу. Рассмотрению этих угроз посвящена лекция 15. Средства, используемые для минимизации возможности успешной реализации этих угроз и обнаружении попыток такой реализации, рассматриваются в лекции 16.

13.3 Классификация мер по обеспечению ИБ

Комплекс мер по обеспечению ИБ КСС включает великое множество разнообразных мер, которое, ввиду его чрезвычайного разнообразия, следует разделить на ряд классов, так что реализация мер каждого класса требует привлечения специалистов в различных областях человеческой деятельности. Вкратце охарактеризуем эти классы мер по обеспечению ИБ.

- ***Правовые (юридические) меры***. Основные меры этого класса определяются Законодательством РФ в области информатизации и ИБ, которое начало формироваться с 1991 года и к 1997 году включало уже 10 основных законов. К числу этих законов, относится, например, закон "Об информации, информатизации и защите информации", принятый 20.02.95 г. В рамках работ над указанным законодательством был существенно дополнен Уголовный кодекс (УК) РФ, в который 1.12.97 г. была включена

глава 28 «Преступления в сфере компьютерной информации». Упомянём лишь три статьи из указанной главы, имеющих непосредственное отношение к проблемам, обсуждаемых в этой заключительной главе настоящей книги. *Статья 272 УК РФ* "Неправомерный доступ к компьютерной информации" позволяет привлечь к уголовной ответственности лиц, осуществляющих (любыми методами) несанкционированный доступ к информации, хранящейся в компонентах КСС и передаваемой по их каналам связи. В соответствии со *ст. 273 УК РФ* "Создание, использование и распространение вредоносных программ для ЭВМ" к уголовной ответственности можно привлечь не только лиц, упомянутых в этой статье, но и лиц, применяющих вполне легальные программы, называемые сканерами безопасности" (см лекцию 15) для анализа "чужих" КСС. А *ст. 474 УК РФ* "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети" является основанием для привлечения к уголовной ответственности, сотрудников нарушающих требования их должностных инструкций а также регламентов, приказов и иных документов, определяющих правила эксплуатации КСС.

К числу юридических мер относятся также меры по надлежащей разработке тех разделов договоров владельца КСС с иными организациями и частными лицами, которые связаны с определением ответственности сторон и порядка разрешения спорных ситуаций.

- ***Экономические меры***. К их числу относятся, например, введение системы коэффициентов и надбавок персоналу, обеспечивающему реализацию мер обеспечения ИБ; страхование оборудования, информации, имущественных и информационных рисков; возмещение убытков и компенсация ущерба.
- ***Организационные меры***. В число основных мер этого класса входят:

  - выбор мест расположения оборудования КС, включая резервные площадки;

  - физическая защита всех компонентов КСС, организация охраны, ограничение доступа в помещения, в которых расположены компоненты КСС (с применением соответствующих технических средств);

  - подбор персонала и работа с персоналом;

  - разработка регламентов и инструкций по обеспечению ИБ, а также контроль их строгого выполнения;

  - организация учета оборудования и носителей информации и надлежащего

хранения носителей;

- выбор партнёров и работа с партнёрами;
- обеспечение надёжного сервисного обслуживания;
- организация взаимодействия с правоохранительными, следственными и судебными органами.

- ***Инженерно-технические меры***. К ним относятся:
  - обеспечение грозозащиты оборудования и зданий;
  - защита помещений от разрушений (включая противопожарную охрану);
  - применение средств визуальной защиты (видеонаблюдения);
  - экранирование помещений от возможных средств внешнего наблюдения;
  - и ряд других мер.
- ***Технические меры*** включают:
  - резервирование технических средств обработки и каналов связи;
  - создание резервных копий (дублирования) файлов и баз данных;
  - использование источников гарантированного электропитания;
  - контроль отсутствия технических средств съема информации;
  - и некоторые другие меры.
- ***Программно-технические меры*** и “объекты” их применения являются предметом разностороннего рассмотрения в последующих лекциях. Именно эти меры предпринимаются для обеспечения ИБ специалистами в области информационно-коммуникационных технологий, а также многими “рядовыми” пользователями компьютерных сетей.

После рассмотрения приведённого перечня мер читателю должно быть ясно, что для решения комплекса разноплановых задач обеспечения ИБ КСС необходимо привлечение специалистов различных профилей, соответствующих различным классам мер по обеспечению ИБ. В наши же дальнейшие задачи входит изучение основ программно-технических угроз ИБ и программно-технических мер борьбы с этими угрозами. К рассмотрению этих вопросов мы перейдём со следующей лекции.

13.4 Понятие о политике ИБ

Достаточно очевидно, что полнообъемная реализация всей рассмотренной в предыдущем пункте совокупности мер, направленных на обеспечение ИБ КСС, является чрезвычайно дорогостоящим мероприятием. Ведь только 100

процентное резервирование всего оборудования и всех каналов вдвое увеличит совершенно не малую стоимость КСС.

Поэтому перед реализацией мер по обеспечению ИБ конкретной КСС необходимо предварительно выработать применяемую *политику ИБ*. Вкратце рассмотрим действия, необходимые для её выработки, подытожив это рассмотрение кратким определением понятия “политика ИБ”.

Для выработки политики ИБ в первую очередь необходимо оценить финансовые риски реализации различных угроз для основных укрупнённых компонентов КСС с учётом вероятности реализации этих угроз и наносимого при такой реализации финансового ущерба. Под укрупнёнными компонентами понимаются такие компоненты как центр обработки данных, компьютеры (с периферийным оборудованием) различных групп пользователей и наиболее важных пользователей, различные каналы передачи данных и пр. Отметим, что оценка финансового ущерба реализации различных угроз может в дальнейшем использоваться при заключении договоров на страхование имущества. *Отметим, что размер убытков от реализации любого из типов угроз может существенно отличаться для КСС организаций различных типов*. Так часовая неработоспособность компьютерной сети учебного заведения может не повлечь никаких прямых финансовых убытков. Аналогичная неработоспособность сети крупного банка может обернуться огромными штрафными санкциями.

Следующим шагом является определение стоимости мер по обеспечению защиты от упомянутых выше угроз и/или ликвидации их последствий (в частности, по возмещению убытков) в случае невозможности предотвращения тех или иных угроз. Отметим, что стоимость программно-технических мер во многом зависит от стоимости требуемого для этого программного обеспечения и может быть существенно снижена за счёт использования свободно-распространяемого ПО. Но в организациях некоторых типов такое ПО может использоваться лишь в случаях, если оно сертифицировано соответствующими органами.

И, наконец, на третьем шаге на основе выработки компромисса между финансовыми рисками угроз ИБ и стоимости мер по предотвращению соответствующих угроз и/или ликвидации их последствий формулируется *политика ИБ*, определяющая состав мер по обеспечению ИБ, обязательных для конкретной рассматриваемой КСС.