КАК ОЦЕНИТЬ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ?

А. В. Соколов, Генеральный директор
С. В. Вихорев, Директор департамента
ОАО «ЭЛВИС-ПЛЮС»

"Технологии и средства связи", №5, 2000

Перед тем, как приступить к созданию системы защиты, всегда встает вопрос: а от чего же надо защититься?

От того, насколько трезво будет дана оценка возникающим угрозам безопасности информации, во многом будет зависеть и выбор оптимального режима защиты.

Данная статья посвящена проблемам оценки угроз безопасности. По мнению авторов, она содержит некий инструмент, позволяющий с определенной степенью достоверности, исходя на первом этапе только из бытового восприятия необходимости защиты информации, не имея большого опыта работы в области защиты информации, определить требуемую степень защиты объекта.

Эта статья будет интересна менеджерам по защите информации, администраторам безопасности информационных систем и топ-менеджерам, отвечающим за безопасность своего учреждения.

Надеемся, что эту статью не оставят без внимания и разработчики средств защиты информации, которым она сможет послужить оценочным материалом при выборе направлений совершенствования средств защиты или создания кооперации для решения поставленных задач.

Зачем все это нужно?

В самом начале надо отметить, что без определенных допущений, так сказать начальных условий, разговор может не получиться. Поэтому лучше сразу оговорим условия. Во-первых, предположим, что у нас действительно есть информация, которую необходимо защищать от посторонних глаз. Во-вторых, мы действительно, здраво рассудив, идем на определенные затраты по созданию системы защиты информации. Правда, нам очень хочется затратить на это как можно меньше средств (как можно меньше - это не значит мало, это ровно столько, сколько объективно требуется для защиты). Для этой цели нам надо выбрать оптимальное соотношение методов защиты, максимально учитывающих уже сделанную какую-никакую работу. Попробуем решить эту задачу со многими неизвестными.

Жизнь современной фирмы невозможно представить без хорошо развитой корпоративной сети, обеспечивающей постоянный обмен деловой информацией независимо от местонахождения пользователей. Обеспечение безопасности деятельности (в широком смысле) любой фирмы реализуется созданием системы защиты - продуманного комплекса мер и средств, направленных на выявление, парирование и ликвидацию различных видов угроз. При этом каждый объект защиты, будь то человек, процесс, средство, имеет свою особую специфику, которая и должна найти свое отражение в общей системе защиты. При этом надо помнить, что одни и те же методы могут быть использованы для парирования различных угроз. Построив железобетонный бункер, мы не только защитим людей от превратностей судьбы, но и обеспечим в какой-то степени целостность информационных процессов.

Об актуальности решения проблемы защиты информации уже сказано достаточно много. Напомним только, что искажение информации, необходимой для принятия ответственных бизнес-решений, блокирование процесса ее получения от партнеров или сотрудников, внедрение в оборот ложной информации, разрушение имеющихся информационных ресурсов, содержащих финансовую, маркетинговую или технологическую информацию, может нанести непоправимый урон деловой репутации фирмы, способствовать принятию ошибочных решений, приводящих к значительному материальному ущербу, а иногда несет и непосредственную угрозу жизни.

Информация, обрабатываемая в корпоративных сетях, особенно уязвима. Существенному повышению возможности несанкционированного использования или модификации информации, введению в оборот ложной информации в настоящее время способствуют:

- увеличение объемов обрабатываемой, передаваемой и хранимой в компьютерах информации;
- сосредоточение в базах данных информации различного уровня важности и конфиденциальности;

- расширение доступа круга пользователей к информации, хранящейся в базах данных, и к ресурсам вычислительной сети;
- увеличение числа удаленных рабочих мест
- широкое использование для связи пользователей глобальной сети Internet и различных каналов связи;
- автоматизация обмена информацией между компьютерами пользователей.

Прежде всего, попробуем определить, что защищать, от кого или от чего защищать и уж потом решить вопрос, как защищать.

Этап первый. Что защищать (модель корпоративной сети).

Основное назначение любой корпоративной сети состоит в обязанности доставить необходимую информацию пользователю, где бы он ни находился и, желательно, в минимально короткий срок. Поэтому, как бы ни желая глобализовать проблему обеспечения защиты информации, необходимо с горечью признать, что эта проблема, при всей ее важности и актуальности всегда была, есть и будет вторичной, то есть вспомогательной проблемой. И как бы ни хотелось разработчику средств защиты информации, система защиты должна не мешать, а, наоборот, способствовать выполнению основной функции - своевременному обмену деловой информацией. К этой проблеме и принципам построения системы защиты мы еще вернемся ниже, а пока будем учитывать, что не корпоративная сеть делается под систему защиты, а система защиты помогает корпоративной сети и является вспомогательной (но очень важной!) системой. Из этого следует, что прежде чем переходить к построению модели системы защиты, необходимо определиться с моделью самой корпоративной сети.

Двух повторяющихся сетей нет. Каждая сеть уникальна по-своему. Поэтому попробуем выделить основные элементы, присущие любой сети и построить достаточно упрощенную (усложнить ее - дело вкуса каждого), но дееспособную модель корпоративной сети, которая бы выполняла все основные функции и содержала бы весь набор элементов, и рассмотреть на ней предмет наших рассуждений.

Что же в общем виде представляет из себя любая корпоративная сеть? (см. рис.1).

Основным объектом вожделения, естественно, является информация, обрабатываемая в корпоративной сети. А информация обрабатывается с помощью специального инструмента - программного обеспечения (ПО). Поэтому базисом любой корпоративной сети является общесистемное программное обеспечение, которое может содержать различные операционные системы, программные оболочки, программы общего назначения, текстовые процессоры, редакторы и интегрированные пакеты программ, системы управления базами данных. Кроме того, для обработки информации используется также прикладное программное обеспечение, то есть такие программы, которые разрабатываются специально для фирмы и в ее интересах для решения специализированных задач.

В процессе обработки информации используются различные технические устройства обработки, хранения и передачи данных. Информация может поступать с автоматизированного рабочего места (АРМ) по внутренним и по внешним каналам связи, при этом информация может вводиться как с клавиатуры, так и с внешних носителей информации. Кроме того, могут использоваться информационные ресурсы других учреждений и организаций и ресурсы глобальных телекоммуникационных сетей. Глобальные телекоммуникационные сети могут так же использоваться в качестве транспортной среды для передачи информации потребителям.

Под понятием "пользователь корпоративной сети" понимается зарегистрированные установленным порядком персоны (организации), наделенные определенными полномочиями доступа в сети. В рамках своих полномочий пользователь может осуществлять только разрешенные ему действия с использованием общесистемного и прикладного ПО.

Обработка информации в сети осуществляется под контролем администраторов системы, а ее защита - администраторов безопасности, которые выполняют свои функции, имея специализированные рабочие места. Эти места не всегда позволяют получить доступ к обрабатываемой информации, но всегда позволяют повлиять на процесс ее обработки, а также – на модернизацию инструмента обработки.

Для разработки прикладного ПО, адаптации общесистемного ПО и поддержания сети в работоспособном состоянии, как правило, привлекаются специалисты-программисты и технический персонал, которые так же имеют ограниченные возможности по доступу к самой информации, но неограниченные возможности по изменению программного обеспечения и процессов обработки информации.

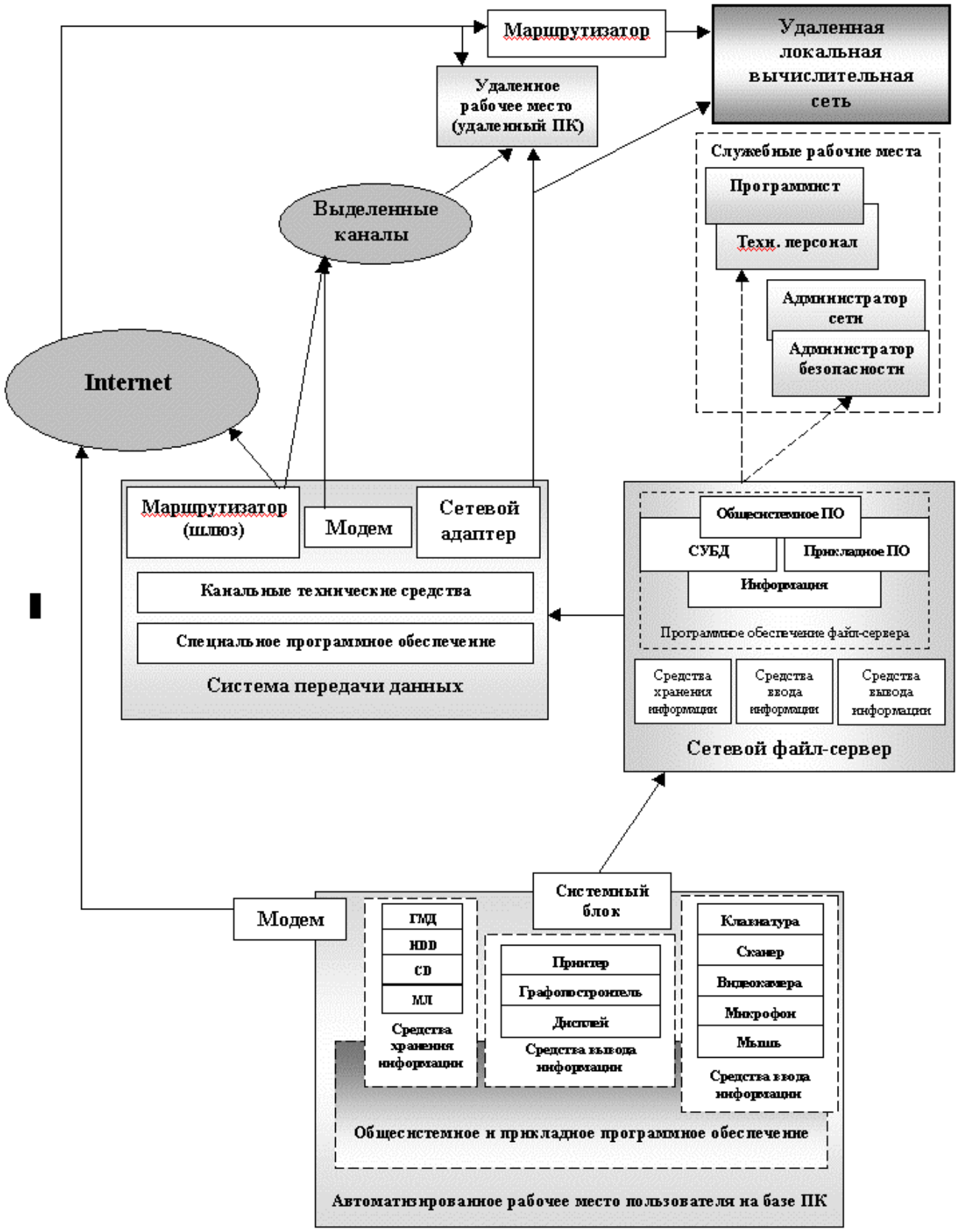

Рис. 1. Модель корпоративной сети

Корпоративную сеть можно представить в виде системы, состоящей из ряда аппаратно-программных подсистем - рабочее место руководителя, удаленное рабочее место, рабочее место администратора безопасности и системы, - каждая из которых является относительно самостоятельной системой. Такой подсистеме присущи признаки общей системы. Поэтому с точки зрения защиты информации, здесь применим принцип декомпозиции. Основываясь на этом принципе, механизм воздействия угроз безопасности информации применим как к системе в целом, так и к отдельной подсистеме. Это очень важный тезис, который позволит в дальнейшем правильно оценить воздействие угроз безопасности информации на отдельные элементы системы, особенно на ее автономные элементы.

Описав, с Божьей помощью, что защищать (объект применения угроз безопасности информации), попробуем перейти к тому, от чего или от кого защищаться, то есть определимся с угрозами безопасности информации, которые могут быть.

Этап второй.
От чего или кого защищаться (модель угроз безопасности).

В литературе, посвященной вопросам защиты информации, можно найти различные варианты моделей угроз безопасности информации. Это объясняется стремлением более точно описать многообразные ситуации воздействия на информацию и определить наиболее адекватные меры парирования. В принципе, можно пользоваться любой понравившейся моделью, необходимо только убедиться, что она описывает максимально большое число факторов, влияющих на безопасность информации. Но, прежде всего, надо помнить, что пользователю, то есть потребителю информации и информационных услуг, оказываемых корпоративной сетью, глубоко без разницы, не получит ли он информацию вовремя, получит ее в искаженном виде или вообще потеряет по вине неправильной работы технических средств, пожара в серверном зале или за счет действий злоумышленника. Итог для него во всех случаях одинаков - понесенные убытки (моральные или материальные).

Что же такое угроза безопасности информации? Это - действие, направленное против объекта защиты, проявляющееся в опасности искажений и потерь информации. Надо оговориться, что речь идет не о всей информации, а только о той ее части, которая, по мнению ее собственника (пользователя), имеет коммерческую ценность (информация как товар) или подлежит защите в силу закона (конфиденциальная информация).

Необходимо также учитывать, что источники угроз безопасности могут находиться как внутри фирмы - внутренние источники, так и вне ее - внешние источники. Такое деление оправдано потому, что для одной и той же угрозы (например, кража) методы парирования для внешних и внутренних источников будут разными.

При составлении модели угроз авторы использовали различные широко используемые в настоящее время варианты моделей, разработанные специалистами в области защиты информации государственных и негосударственных научных учреждений и собственный опыт работы в этой области. Исходя из проведенного анализа, все источники угроз безопасности информации, циркулирующей в корпоративной сети, можно разделить на три основные группы:

I. Угрозы, обусловленные действиями субъекта (антропогенные угрозы)
II. Угрозы, обусловленные техническими средствами (техногенные угрозы)
III. Угрозы, обусловленные стихийными источниками

Первая группа наиболее обширна и представляет наибольший интерес с точки зрения организации парирования этим угрозам, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия этим угрозам управляемы и напрямую зависят от воли организаторов защиты информации.

Субъекты, действия которых могут привести к нарушению безопасности информации, могут быть как внешние:

- криминальные структуры;
- рецидивисты и потенциальные преступники;

- недобросовестные партнеры;
- конкуренты;
- политические противники;

так и внутренние:

- персонал учреждения;
- персонал филиалов;
- лица с нарушенной психикой;
- специально внедренные агенты.

Основываясь на результатах международного и российского опыта, действия субъектов могут привести к ряду нежелательных последствий, среди которых применительно к корпоративной сети, можно выделить следующие:

1. Кража

    - а) технических средств (винчестеров, ноутбуков, системных блоков);
    - б) носителей информации (бумажных, магнитных, оптических и пр.);
    - в) информации (чтение и несанкционированное копирование);
    - г) средств доступа (ключи, пароли, ключевая документация и пр.).

2. Подмена (модификация)

    - а) операционных систем;
    - б) систем управления базами данных;
    - в) прикладных программ;
    - г) информации (данных), отрицание факта отправки сообщений;
    - д) паролей и правил доступа.

3. Уничтожение (разрушение)

    - а) технических средств (винчестеров, ноутбуков, системных блоков);
    - б) носителей информации (бумажных, магнитных, оптических и пр.);
    - в) программного обеспечения (ОС, СУБД, прикладного ПО)
    - г) информации (файлов, данных)
    - д) паролей и ключевой информации.

4. Нарушение нормальной работы (прерывание)

    - а) скорости обработки информации;
    - б) пропускной способности каналов связи;
    - в) объемов свободной оперативной памяти;
    - г) объемов свободного дискового пространства;
    - д) электропитания технических средств;

5. Ошибки

    - а) при инсталляции ПО, ОС, СУБД;
    - б) при написании прикладного ПО;
    - в) при эксплуатации ПО;
    - г) при эксплуатации технических средств.

6. Перехват информации (несанкционированный)

    - а) за счет ПЭМИ от технических средств;

- б) за счет наводок по линиям электропитания;
- в) за счет наводок по посторонним проводникам;
- г) по акустическому каналу от средств вывода;
- д) по акустическому каналу при обсуждении вопросов;
- е) при подключении к каналам передачи информации;
- ж) за счет нарушения установленных правил доступа (взлом).

Вторая группа содержит угрозы менее прогнозируемые, напрямую зависящие от свойств техники и поэтому требующие особого внимания. Технические средства, содержащие потенциальные угрозы безопасности информации, так же могут быть внутренними:

- некачественные технические средства обработки информации;
- некачественные программные средства обработки информации;
- вспомогательные средства (охраны, сигнализации, телефонии);
- другие технические средства, применяемые в учреждении;

и внешними:

- средства связи;
- близко расположенные опасные производства;
- сети инженерных коммуникации (энерго-, водоснабжения, канализации);
- транспорт.

Последствиями применения таких технических средств, напрямую влияющими на безопасность информации, могут быть:

1. Нарушение нормальной работы

- а) нарушение работоспособности системы обработки информации;
- б) нарушение работоспособности связи и телекоммуникаций;
- в) старение носителей информации и средств ее обработки;
- г) нарушение установленных правил доступа;
- д) электромагнитное воздействие на технические средства.

2. Уничтожение (разрушение)

- а) программного обеспечения, ОС, СУБД;
- б) средств обработки информации (броски напряжений, протечки);
- в) помещений
- г) информации (размагничивание, радиация, протечки и пр.);
- д) персонала.

3. Модификация (изменение)

- а) программного обеспечения. ОС, СУБД;
- б) информации при передаче по каналам связи и телекоммуникациям.

Третью группу составляют угрозы, которые совершенно не поддаются прогнозированию, и поэтому меры их парирования должны применяться всегда. Стихийные источники, составляющие потенциальные угрозы информационной безопасности, как правило, являются внешними по отношению к рассматриваемому объекту и под ними понимаются, прежде всего, природные катаклизмы:

- пожары;
- землетрясения;
- наводнения;
- ураганы;

- другие форс-мажорные обстоятельства;
- различные непредвиденные обстоятельства;
- необъяснимые явления.

Эти природные и необъяснимые явления так же влияют на информационную безопасность, опасны для всех элементов корпоративной сети и могут привести к следующим последствиям:

1. Уничтожение (разрушение)

- а) технических средств обработки информации;
- б) носителей информации;
- в) программного обеспечения (ОС, СУБД, прикладного ПО);
- г) информации (файлов, данных);
- д) помещений;
- е) персонала.

2. Исчезновение (пропажа)

- а) информации в средствах обработки;
- б) информации при передаче по телекоммуникационным каналам;
- в) носителей информации;
- г) персонала.

Даже первичный анализ приведенного перечня угроз безопасности информации показывает, что для обеспечения комплексной безопасности необходимо принятие как организационных, так и технических решений парирования. Такой подход позволяет дифференцировано подойти к распределению материальных ресурсов, выделенных на обеспечение информационной безопасности.

Необходимо отметить, что оценить весовые коэффициенты каждой угрозы достаточно затруднительно из-за высокой латентности их проявлений и отсутствия вразумительной статистики по этому вопросу. Поэтому в современной литературе можно найти различные шкалы оценок. Вместе с тем, на основе анализа, проводимого различными специалистами в области компьютерных преступлений, и собственных наблюдений по частоте проявления угрозы безопасности можно расставить так:

- кража (копирование) программного обеспечения
- подмена (несанкционированный ввод) информации
- уничтожение (разрушение) данных на носителях информации
- нарушение нормальной работы (прерывание) в результате вирусных атак
- модификация (изменение) данных на носителях информации
- перехват (несанкционированный съем) информации
- кража (несанкционированное копирование) ресурсов
- нарушение нормальной работы (перегрузка) каналов связи
- непредсказуемые потери.

Несмотря на предложенную градацию (примем ее только к сведению), для простоты будем считать, что каждая угроза может себя рано или поздно проявить, и поэтому все они равны, то есть при построении модели принято, что весовые коэффициенты каждой угрозы равны 1.

Описав состав угроз безопасности информации, мы еще не решили проблемы моделирования их воздействия. Все эти угрозы по-разному проявляются в каждой точке корпоративной сети. Поэтому попробуем оценить, исходя из обычной логики и собственного опыта, в какой точке какая угроза представляет наибольшую опасность. (см. рис.2).

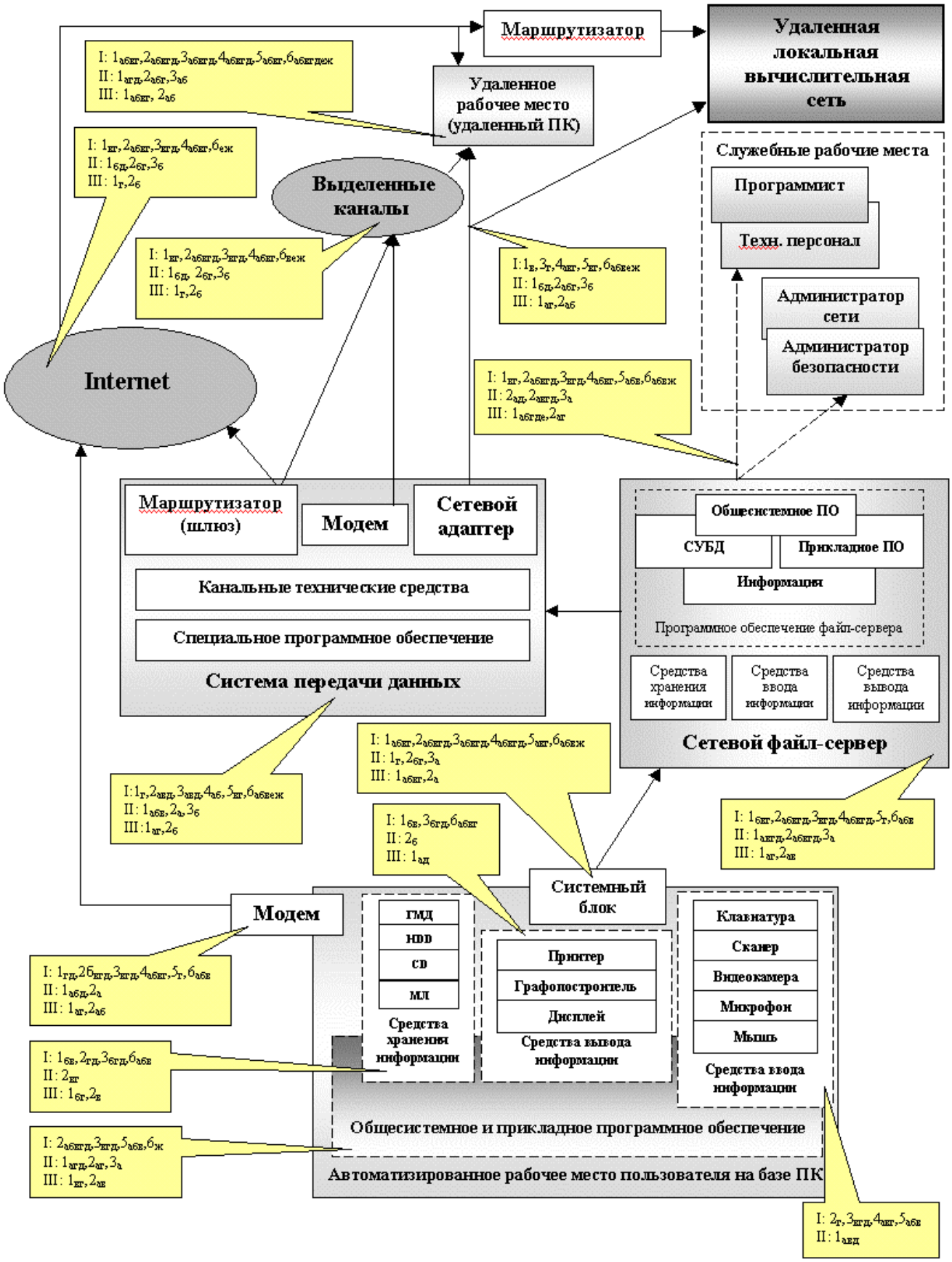

Рис. 2. Модель угроз безопасности информации корпоративной сети

Наложение угроз безопасности информации на модель корпоративной сети позволяет в первом приближении оценить их опасность и методом исключения определить наиболее актуальные для конкретного объекта защиты. Кроме того, можно в первом приближении оценить объемы необходимых работ и выбрать магистральное направление по обеспечению защиты информации.

Следствием реализации выявленных угроз безопасности информации, в конечном счете, может стать ущемление прав собственника (пользователя) информации или нанесение ему материального ущерба, наступившее в результате:

- **уничтожения информации** из-за нарушения программных, аппаратных или программно-аппаратных средств ее обработки или систем защиты, форс-мажорных обстоятельств, применения специальных технических (например, размагничивающих генераторов), программных (например, логических бомб) средств воздействия, осуществляемого конкурентами, персоналом учреждения или его филиалов, преступными элементами или поставщиками средств обработки информации в интересах третьих лиц;
- **модификации или искажения информации** вследствие нарушения программных, аппаратных или программно-аппаратных средств ее обработки или систем защиты, форс-мажорных обстоятельств, применения специальных программных (например, лазеек) средств воздействия, осуществляемого конкурентами, персоналом учреждения, поставщиками средств обработки информации в интересах третьих лиц;
- **хищения информации** путем подключения к линиям связи или техническим средствам, за счет снятия и расшифровки сигналов побочных электромагнитных излучений, фотографирования, кражи носителей информации, подкупа или шантажа персонала учреждения или его филиалов, прослушивания конфиденциальных переговоров, осуществляемого конкурентами, персоналом учреждения или преступными элементами, несанкционированного копирования информации, считывания данных других пользователей, мистификации (маскировки под запросы системы), маскировки под зарегистрированного пользователя, проводимых обслуживающим персоналом автоматизированной системы, хищение информации с помощью программных ловушек;
- **махинаций с информацией** путем применения программных, программно-аппаратных или аппаратных средств, осуществляемых в интересах третьих лиц поставщиками средств обработки информации или проводимых персоналом учреждения, а также путем подделки электронной подписи или отказа от нее.

Итак, теперь мы знаем, что и от кого или чего надо защищать. Попробуем разобраться с тем, как защищать.

Этап третий.
Как защищаться (модель парирования угрозам безопасности).

Уменьшить отрицательное воздействие угроз безопасности информации возможно различными методами. Среди таких методов можно выделить четыре основных группы:

- Организационные методы;
- Инженерно-технические методы;
- Технические методы;
- Программно-аппаратные методы.

Организационные методы, в основном, ориентированы на работу с персоналом, выбор местоположения и размещения объектов корпоративной сети, организацию систем физической и противопожарной защиты, организацию контроля выполнения принятых мер, возложение персональной ответственности за выполнение мер защиты. Эти методы применяются не только для защиты информации и, как правило, уже частично реализованы на объектах корпоративной сети. Однако, их применение дает значительный эффект и сокращает общее число угроз.

Инженерно-технические методы связаны с построением оптимальных сетей инженерных коммуникаций с учетом требований безопасности информации. Это довольно дорогостоящие методы, но они, как правило, реализуются еще на этапе строительства или реконструкции объекта, способствуют повышению его общей живучести и дают высокий эффект при устранении некоторых угроз безопасности информации. Некоторые источники угроз, например обусловленные стихийными бедствиями или техногенными факторами, вообще не устранимы другими методами.

Технические методы основаны на применении специальных технических средств защиты информации и контроля обстановки и дают значительный эффект при устранении угроз безопасности информации, связанных с действиями криминогенных элементов по добыванию информации незаконными техническими

средствами. Кроме того, некоторые методы, например, резервирование средств и каналов связи, оказывают эффект при некоторых техногенных факторах.

Программно-аппаратные методы, в основном, нацелены на устранение угроз, непосредственно связанных с процессом обработки и передачи информации. Без этих методов невозможно построение целостной комплексной системы информационной безопасности.

Сопоставим описанные выше угрозы безопасности информации и группы методов их парирования. Это позволит определить, какими же методами какие угрозы наиболее целесообразно парировать, и определить соотношение в распределении средств, выделенных на обеспечение безопасности информации между группами методов.

Анализ результатов моделирования с учетом принятых в модели ограничений и допущений позволяет сказать, что все группы методов парирования угрозам безопасности информации имеют примерно равную долю в организации комплексной защиты информации. Однако, необходимо учесть, что некоторые методы могут быть использованы только для решения ограниченного круга задач защиты. Это особенно характерно для устранения угроз техногенного и стихийного характера.

Наибольший эффект достигается при применении совокупности организационных и программно-аппаратных методов парирования. Анализ весовых коэффициентов программно-аппаратных методов позволяет сделать вывод, что гипотетическое средство защиты корпоративной сети, прежде всего, должно обеспечивать разграничение доступа субъектов к объектам (мандатный и дискреционный принципы), управлять внешними потоками информации (фильтрация, ограничение, исключение) и, как минимум, обеспечивать управление внутренними потоками информации с одновременным контролем целостности программного обеспечения, конфигурации сети и возможности атак разрушающих воздействий.

Немного философии.

Наконец мы определились, что, от кого и как защищать. Пора переходить к созданию системы комплексной защиты информации корпоративной сети. Здесь каждый волен выбирать сам, как эту систему строить. Надеемся, что этот материал поможет правильно оценить обстановку и выбрать пути реализации. Но прежде чем переходить к этому этапу, хотелось бы обратить Ваше внимание на некоторые моменты, без которых построенная система комплексной защиты будет не только бесполезна, но и вредна. Поговорим немного о принципах построения таких систем и вспомним основные из них.

Парирование угрозам безопасности информации всегда носит недружественный характер по отношению к пользователям и обслуживающему персоналу корпоративной сети. Это происходит из-за того, что любая система защиты, по определению, всегда налагает ограничения на работу организационного и технического характера.

Поэтому одним из основных принципов создания системы комплексной защиты информации должен стать **принцип максимальной дружественности**. То есть не надо вводить запреты там, где без них можно обойтись ("на всякий случай"), а если уж и вводить ограничения, то перед этим посмотреть, как это можно сделать с минимальными неудобствами для пользователя. При этом следует учесть не только совместимость создаваемой системы комплексной защиты с используемой операционной и программно-аппаратной структурой корпоративной сети и сложившимися традициями фирмы.

Вплотную к этой проблеме стоит **принцип прозрачности**. Корпоративной сетью пользуются не только высококлассные программисты. Кроме того, основное назначение корпоративной сети является обеспечение производственных потребностей пользователей, то есть - работа с информацией. Поэтому система защиты информации должна работать в "фоновом" режиме, быть "незаметной" и не мешать пользователям в основной работе, но при этом выполнять все возложенные на нее функции.

Принцип превентивности. Надо всегда помнить, что устранение последствий проявления угроз безопасности информации потребует значительных финансовых, временных и материальных затрат, гораздо больших, чем затраты на создание системы комплексной защиты информации.

Принцип оптимальности. Оптимальный выбор соотношения между различными методами и способами парирования угрозам безопасности информации при принятии решения позволит в значительной степени сократить расходы на создание системы защиты информации.

Принцип адекватности. Принимаемые решения должны быть дифференцированы в зависимости от важности, частоты и вероятности возникновения угроз безопасности информации, степени конфиденциальности самой информации и ее коммерческой стоимости.

Принцип системного подхода к построению системы защиты позволяет заложить комплекс мероприятий по парированию угрозам безопасности информации уже на стадии проектирования корпоративной сети, обеспечив оптимальное сочетание организационных и инженерно-технических мер защиты информации. Важность реализации этого принципа основана на том, что оборудование действующей незащищенной корпоративной сети средствами защиты информации сложнее и дороже, чем изначальное проектирование и построение ее в защищенном варианте.

Принцип адаптивности. Система защиты информации должна строиться с учетом возможного изменения конфигурации сети, числа пользователей и степени конфиденциальности и ценности информации. При этом, введение каждого нового элемента сети или изменение действующих условий не должно снижать достигнутый уровень защищенности корпоративной сети в целом.

Принцип доказательности. При создании системы защиты информации необходимо соблюдение организационных мер внутри корпоративной сети, включая привязку логического и физического рабочих мест друг к другу, и применения специальных аппаратно-программных средств идентификации, аутентификации и подтверждения подлинности информации. Реализация данного принципа позволяет сократить расходы на усложнение системы, например, применять цифровую электронную подпись только при работе с удаленными и внешними рабочими местами и терминалами, связанными с корпоративной сетью по каналам связи.

Эти принципы должны быть положены в основу при выборе направлений обеспечения безопасности корпоративной сети, функций и мер защиты информации.

В завершении несколько слов вот о чем. Определившись с функциями, которые должны быть реализованы для защиты информации на конкретном объекте и приступая к выбору конкретных технических решений, то есть к выбору средств защиты информации, обязательно встает вопрос о подтверждении выполнения тех или иных функций конкретным средством защиты. Это немаловажный процесс, который в определенных случаях, (например при организации защиты информации, содержащей государственную тайну или сведения о личности - персональные данные) строго регламентирован. Что же может явиться свидетельством того, что те или иные функции защиты реализованы конкретным средством защиты? Конечно же сертификат соответствия - документ, которым независимые эксперты свидетельствуют о готовности средства выполнить эти функции.
