Лекция 1
Сетевая безопасность

1. Основные понятия безопасности
2. Конфиденциальность, целостность и доступность данных
3. Классификация угроз
4. Системный подход к обеспечению безопасности
5. Политика безопасности
6. Вопросы

1. Основные понятия безопасности

При рассмотрении безопасности информационных систем обычно выделяют две группы проблем:

- безопасность компьютера
- сетевая безопасность.

К *безопасности компьютера* относят все проблемы защиты данных, хранящихся и обрабатывающихся компьютером, который рассматривается как автономная система. Эти проблемы решаются средствами операционных систем и приложений, таких как базы данных, а также встроенными аппаратными средствами компьютера.

Под *сетевой безопасностью* понимают все вопросы, связанные с взаимодействием устройств в сети, это прежде всего защита данных в момент их передачи по линиям связи и защита от несанкционированного удаленного доступа в сеть. И хотя подчас проблемы компьютерной и сетевой безопасности трудно отделить друг от друга, настолько тесно они связаны, совершенно очевидно, что сетевая безопасность имеет свою специфику.

Автономно работающий компьютер можно эффективно защитить от внешних покушений разнообразными способами, например просто запереть на замок клавиатуру или снять жесткий накопитель и поместить его в сейф. Компьютер, работающий в сети, по определению не может полностью отгородиться от мира, он должен общаться с другими компьютерами, возможно, даже удаленными от него на большое расстояние, поэтому обеспечение безопасности в сети является задачей значительно более сложной.

Логический вход чужого пользователя в ваш компьютер является штатной ситуацией, если вы работаете в сети. Обеспечение безопасности в такой ситуации сводится к тому, чтобы сделать это проникновение контролируемым — каждому пользователю сети должны быть четко определены его права по доступу к информации, внешним устройствам и выполнению системных действий на каждом из компьютеров сети.

Помимо проблем, порождаемых возможностью удаленного входа в сетевые компьютеры, сети по своей природе подвержены еще одному виду опасности — перехвату и анализу сообщений, передаваемых по сети, а также созданию «ложного» графика. Большая часть средств обеспечения сетевой безопасности направлена на предотвращение именно этого типа нарушений.

Вопросы сетевой безопасности приобретают особое значение сейчас, когда при построении корпоративных сетей наблюдается переход от использования выделенных каналов к публичным сетям (Интернет, frame relay). Поставщики услуг публичных сетей пока редко обеспечивают защиту пользовательских данных при их транспортировке по своим магистралям, возлагая на пользователей заботы по их конфиденциальности, целостности и доступности.

2. Конфиденциальность, целостность и доступность данных

Безопасная информационная система — это система, которая, во-первых, защищает данные от несанкционированного доступа, во-вторых, всегда готова предоставить их своим пользователям, а в-третьих, надежно хранит информацию и гарантирует неизменность данных. Таким образом, безопасная система по определению обладает свойствами конфиденциальности, доступности и целостности.

- *Конфиденциальность (confidentiality)* — гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен (такие пользователи называются авторизованными).
- *Доступность (availability)* — гарантия того, что авторизованные пользователи всегда получат доступ к данным.
- *Целостность (integrity)* — гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.

Требования безопасности могут меняться в зависимости от назначения системы, характера используемых данных и типа возможных угроз. Трудно представить систему, для которой были бы не важны свойства целостности и доступности, но свойство конфиденциальности не всегда является обязательным. Например, если вы публикуете информацию в Интернете на Web-сервере и вашей целью является сделать ее доступной для самого широкого круга людей, то конфиденциальность в данном случае не требуется. Однако требования целостности и доступности остаются актуальными.

Действительно, если вы не предпримете специальных мер по обеспечению целостности данных, злоумышленник может изменить данные на вашем сервере и нанести этим ущерб вашему предприятию. Преступник может, например, внести такие изменения в помещенный на Web-сервере прайс-лист, которые снизят конкурентоспособность вашего предприятия, или испортить коды свободно распространяемого вашей фирмой программного продукта, что безусловно скажется на ее деловом имидже.

Не менее важным в данном примере является и обеспечение доступности данных. Затратив немалые средства на создание и поддержание сервера в Интернете, предприятие вправе рассчитывать на отдачу: увеличение числа клиентов, количества продаж и т. д. Однако существует вероятность того, что злоумыщленник предпримет атаку, в результате которой помещенные на сервер данные станут недоступными для тех, кому они предназначались. Примером таких злонамеренных действий может служить «бомбардировка» сервера IP-пакетами с неправильным обратным адресом, которые в соответствии с логикой работы этого протокола могут вызывать тайм-ауты, а в конечном счете сделать сервер недоступным для всех остальных запросов.

Понятия конфиденциальности, доступности и целостности могут быть определены не только по отношению к информации, но и к другим ресурсам вычислительной сети, например внешним устройствам или приложениям. Существует множество системных ресурсов, возможность «незаконного» использования которых может привести к нарушению безопасности системы. Например, неограниченный доступ к устройству печати позволяет злоумышленнику получать копии распечатываемых документов, изменять параметры настройки, что может привести к изменению очередности работ и даже к выводу устройства из строя. Свойство конфиденциальности, примененное к устройству печати, можно интерпретировать так, что доступ к устройству имеют те и только те пользователи, которым этот доступ разрешен, причем они могут выполнять только те операции с устройством, которые для них определены. Свойство доступности устройства означает его готовность к использованию всякий раз, когда в этом возникает необходимость. А свойство целостности может быть определено как свойство неизменности параметров настройки данного устройства. Легальность использования сетевых устройств важна не только постольку, поскольку она влияет на безопасность данных. Устройства могут предоставлять различные услуги: распечатку текстов, отправку факсов, доступ в Интернет, электронную почту и т.п., незаконное потребление которых,

наносящее материальный ущерб предприятию, также является нарушением безопасности системы.

Любое действие, которое направлено на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов сети, называется *угрозой.* Реализованная угроза называется *атакой. Риск* — это вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки. *Значение риска тем выше, чем более уязвимой является существующая система безопасности и чем выше вероятность реализации атаки.*

3. Классификация угроз

Универсальной классификации угроз не существует, возможно, и потому, что нет предела творческим способностям человека, и каждый день применяются новые способы незаконного проникновения в сеть, разрабатываются новые средства мониторинга сетевого графика, появляются новые вирусы, находятся новые изъяны в существующих программных и аппаратных сетевых продуктах. В ответ на это разрабатываются все более изощренные средства защиты, которые ставят преграду на пути многих типов угроз, но затем сами становятся новыми объектами атак.

Угрозы могут быть разделены на:

- умышленные
- неумышленные.

Неумышленные угрозы вызываются ошибочными действиями лояльных сотрудников, становятся следствием их низкой квалификации или безответственности. Кроме того, к такому роду угроз относятся последствия ненадежной работы программных и аппаратных средств системы. Так, например, из-за отказа диска, контроллера диска или всего файлового сервера могут оказаться недоступными данные, критически важные для работы предприятия. Поэтому вопросы безопасности так тесно переплетаются с вопросами надежности, отказоустойчивости технических средств. Угрозы безопасности, которые вытекают из ненадежности работы программно-аппаратных средств, предотвращаются путем их совершенствования, использования резервирования на уровне аппаратуры (RAID-массивы, многопроцессорные компьютеры, источники бесперебойного питания, кластерные архитектуры) или на уровне массивов данных (тиражирование файлов, резервное копирование).

Умышленные угрозы могут ограничиваться либо пассивным чтением данных или мониторингом системы, либо включать в себя активные действия, например нарушение целостности и доступности информации, приведение в нерабочее состояние приложений и устройств. Так, умышленные угрозы возникают в результате деятельности хакеров и явно направлены на нанесение ущерба предприятию.

В вычислительных сетях можно выделить следующие типы умышленных угроз:

- незаконное проникновение в один из компьютеров сети под видом легального пользователя;
- разрушение системы с помощью программ-вирусов;
- нелегальные действия легального пользователя;
- «подслушивание» внутрисетевого графика.

Незаконное проникновение может быть реализовано через уязвимые места в системе безопасности с использованием недокументированных возможностей операционной системы. Эти возможности могут позволить злоумышленнику «обойти» стандартную процедуру, контролирующую вход в сеть.

Другим способом незаконного проникновения в сеть является использование «чужих» паролей, полученных путем подглядывания, расшифровки файла паролей, подбора паролей или получения пароля путем анализа сетевого графика. Особенно опасно проникновение злоумышленника под именем пользователя, наделенного большими

полномочиями, например администратора сети. Для того чтобы завладеть паролем администратора, злоумышленник может попытаться войти в сеть под именем простого пользователя. Поэтому очень важно, чтобы все пользователи сети сохраняли свои пароли в тайне, а также выбирали их так, чтобы максимально затруднить угадывание.

Подбор паролей злоумышленник выполняет с использованием специальных программ, которые работают путем перебора слов из некоторого файла, содержащего большое количество слов. Содержимое файла-словаря формируется с учетом психологических особенностей человека, которые выражаются в том, что человек выбирает в качестве пароля легко запоминаемые слова или буквенные сочетания.

Еще один способ получения пароля — это внедрение в чужой компьютер «троянского коня». Так называют резидентную программу, работающую без ведома хозяина данного компьютера и выполняющую действия, заданные злоумышленником. В частности, такого рода программа может считывать коды пароля, вводимого пользователем во время логического входа в систему.

Программа-«троянский конь» всегда маскируется под какую-нибудь полезную утилиту или игру, а производит действия, разрушающие систему. По такому принципу действуют и *программы-вирусы,* отличительной особенностью которых является способность «заражать» другие файлы, внедряя в них свои собственные копии. Чаще всего вирусы поражают исполняемые файлы. Когда такой исполняемый код загружается в оперативную память для выполнения, вместе с ним получает возможность исполнить свои вредительские действия вирус. Вирусы могут привести к повреждению или даже полной утрате информации.

Нелегальные действия легального пользователя — этот тип угроз исходит от легальных пользователей сети, которые, используя свои полномочия, пытаются выполнять действия, выходящие за рамки их должностных обязанностей. Например, администратор сети имеет практически неограниченные права на доступ ко всем сетевым ресурсам. Однако на предприятии может быть информация, доступ к которой администратору сети запрещен. Для реализации этих ограничений могут быть предприняты специальные меры, такие, например, как шифрование данных, но и в этом случае администратор может попытаться получить доступ к ключу. Нелегальные действия может попытаться предпринять и обычный пользователь сети. Существующая статистика говорит о том, что едва ли не половина всех попыток нарушения безопасности системы исходит от сотрудников предприятия, которые как раз и являются легальными пользователями сети.

Подслушивание внутрисетевого трафика — это незаконный мониторинг сети, захват и анализ сетевых сообщений. Существует много доступных программных и аппаратных анализаторов трафика, которые делают эту задачу достаточно тривиальной. Еще более усложняется защита от этого типа угроз в сетях с глобальными связями. Глобальные связи, простирающиеся на десятки и тысячи километров, по своей природе являются менее защищенными, чем локальные связи (больше возможностей для прослушивания трафика, более удобная для злоумышленника позиция при проведении процедур аутентификации). Такая опасность одинаково присуща всем видам территориальных каналов связи и никак не зависит от того, используются собственные, арендуемые каналы или услуги общедоступных территориальных сетей, подобных Интернету.

Однако использование общественных сетей (речь в основном идет об Интернете) еще более усугубляет ситуацию. Действительно, использование Интернета добавляет к опасности перехвата данных, передаваемых по линиям связи, опасность несанкционированного входа в узлы сети, поскольку наличие огромного числа хакеров в Интернете увеличивает вероятность попыток незаконного проникновения в компьютер. Это представляет постоянную угрозу для сетей, подсоединенных к Интернету.

Интернет сам является целью для разного рода злоумышленников. Поскольку Интернет создавался как открытая система, предназначенная для свободного обмена

информацией, совсем не удивительно, что практически все протоколы стека TCP/IP имеют «врожденные» недостатки защиты. Используя эти недостатки, злоумышленники все чаще предпринимают попытки несанкционированного доступа к информации, хранящейся на узлах Интернета.

4. Системный подход к обеспечению безопасности

Построение и поддержка безопасной системы требует системного подхода. В соответствии с этим подходом прежде всего необходимо осознать весь спектр возможных угроз для конкретной сети и для каждой из этих угроз продумать тактику ее отражения. В этой борьбе можно и нужно использовать самые разноплановые средства и приемы — морально-этические и законодательные, административные и психологические, защитные возможности программных и аппаратных средств сети.

К *морально-этическим* средствам защиты можно отнести всевозможные нормы, которые сложились по мере распространения вычислительных средств в той или иной стране. Например, подобно тому как в борьбе против пиратского копирования программ в настоящее время в основном используются меры воспитательного плана, необходимо внедрять в сознание людей аморальность всяческих покушений на нарушение конфиденциальности, целостности и доступности чужих информационных ресурсов.

Законодательные средства защиты — это законы, постановления правительства и указы президента, нормативные акты и стандарты, которыми регламентируются правила использования и обработки информации ограниченного доступа, а также вводятся меры ответственности за нарушения этих правил. Правовая регламентация деятельности в области защиты информации имеет целью защиту информации, составляющей государственную тайну, обеспечение прав потребителей на получение качественных продуктов, защиту конституционных прав граждан на сохранение личной тайны, борьбу с организованной преступностью.

Административные меры — это действия, предпринимаемые руководством предприятия или организации для обеспечения информационной безопасности. К таким мерам относятся конкретные правила работы сотрудников предприятия, например режим работы сотрудников, их должностные инструкции, строго определяющие порядок работы с конфиденциальной информацией на компьютере. К административным мерам также относятся правила приобретения предприятием средств безопасности. Представители администрации, которые несут ответственность за защиту информации, должны выяснить, насколько безопасным является использование продуктов, приобретенных у зарубежных поставщиков. Особенно это касается продуктов, связанных с шифрованием. В таких случаях желательно проверить наличие у продукта сертификата, выданного российскими тестирующими организациями.

Психологические меры безопасности могут играть значительную роль в укреплении безопасности системы. Пренебрежение учетом психологических моментов в неформальных процедурах, связанных с безопасностью, может привести к нарушениям защиты. Рассмотрим, например, сеть предприятия, в которой работает много удаленных пользователей. Время от времени пользователи должны менять пароли (обычная практика для предотвращения их подбора). В данной системе выбор паролей осуществляет администратор. В таких условиях злоумышленник может позвонить администратору по телефону и от имени легального пользователя попробовать получить пароль. При большом количестве удаленных пользователей не исключено, что такой простой психологический прием может сработать.

К *физическим* средствам защиты относятся экранирование помещений для защиты от излучения, проверка поставляемой аппаратуры на соответствие ее спецификациям и отсутствие аппаратных «жучков», средства наружного наблюдения, устройства, блокирующие физический доступ к отдельным блокам компьютера, различные замки и

другое оборудование, защищающие помещения, где находятся носители информации, от незаконного проникновения и т. д. и т. п.

Технические средства информационной безопасности реализуются программным и аппаратным обеспечением вычислительных сетей. Такие средства, называемые также службами сетевой безопасности, решают самые разнообразные задачи по защите системы, например контроль доступа, включающий процедуры аутентификации и авторизации, аудит, шифрование информации, антивирусную защиту, контроль сетевого графика и много других задач. Технические средства безопасности могут быть либо встроены в программное (операционные системы и приложения) и аппаратное (компьютеры и коммуникационное оборудование) обеспечение сети, либо реализованы в виде отдельных продуктов, созданных специально для решения проблем безопасности.

5. Политика безопасности

Важность и сложность проблемы обеспечения безопасности требует выработки *политики информационной безопасности,* которая подразумевает ответы на следующие вопросы:

- Какую информацию защищать?
- Какой ущерб понесет предприятие при потере или при раскрытии тех или иных данных?
- Кто или что является возможным источником угрозы, какого рода атаки на безопасность системы могут быть предприняты?
- Какие средства использовать для защиты каждого вида информации?

Специалисты, ответственные за безопасность системы, формируя политику безопасности, должны учитывать несколько базовых принципов.

Одним из таких принципов является предоставление каждому сотруднику предприятия того *минимально уровня привилегий* на доступ к данным, который необходим ему для выполнения его должностных обязанностей. Учитывая, что большая часть нарушений в области безопасности предприятий исходит именно от собственных сотрудников, важно ввести четкие ограничения для всех пользователей сети, не наделяя их излишними возможностями.

Следующий принцип — использование *комплексного подхода* к обеспечению безопасности. Чтобы затруднить злоумышленнику доступ к данным, необходимо предусмотреть самые разные средства безопасности, начиная с организационно-административных запретов и кончая встроенными средствами сетевой аппаратуры. Административный запрет на работу в воскресные дни ставит потенциального нарушителя под визуальный контроль администратора и других пользователей, физические средства защиты (закрытые помещения, блокировочные ключи) ограничивают непосредственный контакт пользователя только приписанным ему компьютером, встроенные средства сетевой ОС (система аутентификации и авторизации) предотвращают вход в сеть нелегальных пользователей, а для легального пользователя ограничивают возможности только разрешенными для него операциями (подсистема аудита фиксирует его действия). Такая система защиты с многократным резервированием средств безопасности увеличивает вероятность сохранности данных.

Используя многоуровневую систему защиты, важно обеспечивать *баланс надежности защиты всех уровней.* Если в сети все сообщения шифруются, но ключи легкодоступны, то эффект от шифрования нулевой. Или если на компьютерах установлена файловая система, поддерживающая избирательный доступ на уровне отдельных файлов, но имеется возможность получить жесткий диск и установить его на другой машине, то все достоинства средств защиты файловой системы сводятся на нет. Если внешний трафик сети, подключенной к Интернету, проходит через мощный брандмауэр, но пользователи имеют возможность связываться с узлами Интернета по коммутируемым линиям,

используя локально установленные модемы, то деньги (как правило, немалые), потраченные на брандмауэр, можно считать выброшенными на ветер.

Следующим универсальным принципом является использование средств, которые при отказе переходят в состояние *максимальной защиты.* Это касается самых различных средств безопасности. Если, например, автоматический пропускной пункт в какое-либо помещение ломается, то он должен фиксироваться в таком положении, чтобы ни один человек не мог пройти на защищаемую территорию. А если в сети имеется устройство, которое анализирует весь входной трафик и отбрасывает кадры с определенным, заранее заданным обратным адресом, то при отказе оно должно полностью блокировать вход в сеть. Неприемлемым следовало бы признать устройство, которое бы при отказе пропускало в сеть весь внешний трафик.

Принцип единого контрольно-пропускного пункта — весь входящий во внутреннюю сеть и выходящий во внешнюю сеть трафик должен проходить через единственный узел сети, например через межсетевой экран (firewall). Только это позволяет в достаточной степени контролировать трафик. В противном случае, когда в сети имеется множество пользовательских станций, имеющих независимый выход во внешнюю сеть, очень трудно скоординировать правила, ограничивающие права пользователей внутренней сети по доступу к серверам внешней сети и обратно — права внешних клиентов по доступу к ресурсам внутренней сети.

Принцип баланса возможного ущерба от реализации угрозы и затрат на ее предотвращение. Ни одна система безопасности не гарантирует защиту данных на уровне 100 %, поскольку является результатом компромисса между возможными рисками и возможными затратами. Определяя политику безопасности, администратор должен взвесить величину ущерба, которую может понести предприятие в результате нарушения защиты данных, и соотнести ее с величиной затрат, требуемых на обеспечение безопасности этих данных. Так, в некоторых случаях можно отказаться от дорогостоящего межсетевого экрана в пользу стандартных средств фильтрации обычного маршрутизатора, в других же можно пойти на беспрецедентные затраты. Главное, чтобы принятое решение было обосновано экономически.

При определении политики безопасности для сети, имеющей выход в Интернет, специалисты рекомендуют разделить задачу на две части: выработать политику доступа к сетевым службам Интернета и выработать политику доступа к ресурсам внутренней сети компании.

Политика доступа к сетевым службам Интернета включает следующие пункты:

1. Определение списка служб Интернета, к которым пользователи внутренней сети должны иметь ограниченный доступ.
2. Определение ограничений на методы доступа, например на использование протоколов SLIP (Serial Line Internet Protocol) и PPP (Point-to-Point Protocol). Ограничения методов доступа необходимы для того, чтобы пользователи не могли обращаться к «запрещенным» службам Интернета обходными путями. Например, если для ограничения доступа к Интернету в сети устанавливается специальный шлюз, который не дает возможности пользователям работать в системе WWW, они могут устанавливать с Web-серверами PPP-соединения по коммутируемой линии. Во избежание этого надо просто запретить использование протокола PPP.
3. Принятие решения о том, разрешен ли доступ внешних пользователей из Интернета во внутреннюю сеть. Если да, то кому. Часто доступ разрешают только для некоторых, абсолютно необходимых для работы предприятия служб, например электронной почты.

Политика доступа к ресурсам внутренней сети компании может быть выражена в одном из двух принципов:

- запрещать все, что не разрешено в явной форме;

- разрешать все, что не запрещено в явной форме.

В соответствии с выбранным принципом определяются правила обработки внешнего графика межсетевыми экранами или маршрутизаторами. Реализация защиты на основе первого принципа дает более высокую степень безопасности, однако при этом могут возникать большие неудобства у пользователей, а кроме того, такой способ защиты обойдется значительно дороже. При реализации второго принципа сеть окажется менее защищенной, однако пользоваться ею будет удобнее и потребуется меньше затрат.

Вопросы

1. Что относится к безопасности компьютера?
2. Что понимается под сетевой безопасностью?
3. Дайте определение безопасной информационной системе. Какими свойствами она обладает?
4. Что называется угрозой?
5. Что называется атакой?
6. Что такое «риск»?
7. Охарактеризуйте умышленную угрозу, неумышленную.
8. Перечислите типы умышленных угроз.
9. Перечислите средства защиты сетевой безопасности.
10. На какие вопросы подразумевает ответы политика информационной безопасности?
11. Какие принципы нужно учитывать при формировании политики информационной безопасности?
12. Какие пункты включает в себя политика доступа к сетевым службам Интернета?