**Лекция 7:**

**Защита информации в информационных системах и компьютерных сетях**

**Аннотация:**В лекции рассказывается о методологии обеспечения безопасности систем и сетей предприятия

Существование и развитие информационного общества на современном этапе невозможно без использования информационных сетей, глобальных компьютерных сетей и сетей связи — радио, телевидения, фиксированных и мобильных телефонных сетей, *Internet* и т.д. В связи с этим обеспечение доверия и безопасности невозможно без предъявления к этим сетям не только требований по обеспечению надёжности передачи данных, стабильности работы, качества и масштабов охвата, но и по обеспечению информационной безопасности.

Информационная *безопасность* сетей представляет собой "состояние защищённости сбалансированных интересов производителей информационно-коммуникационных технологий и конкретно сетей, потребителей, операторов и органов государственной власти в информационной сфере. В свою *очередь* информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования отношений, возникающих при использовании сетей связи" [материалы Международного конгресса "*Доверие* и *безопасность* в информационном обществе", 21 апреля 2003 г., <http://www.rans.ru/arrangements/int_cong_doc.doc>].

Благодаря своей открытости и общедоступности *компьютерные сети* и сети связи общего пользования являются удобным средством для обеспечения взаимодействия граждан, бизнеса и органов государственной власти. Однако чем более открыты сети, тем более они уязвимы. Можно выделить ряд особенностей, которые делают сети уязвимыми, а нарушителей — практически неуловимыми:

* возможность действия нарушителей на расстоянии в сочетании с возможностью сокрытия своих истинных персональных данных (указанная особенность характерна, в частности, для сети Internet, радиосетей, сетей кабельного телевидения, незаконного использования ресурсов телефонных сетей);
* возможность пропаганды и распространения средств нарушения сетевой безопасности (например, распространение в Internet программных средств, позволяющих реализовывать несанкционированный доступ к информационным ресурсам, нарушать авторские права и т.д.);
* возможность многократного повторения атакующих сеть воздействий (например, генерация в Internet или телефонных сетях потоков вызовов, приводящих к нарушению функционирования узлов сети).

Большинство владельцев и операторов принимают необходимые меры по обеспечению информационной безопасности своих сетей. В то же время, для современного состояния информационной безопасности сетей характерны следующие причины, приводящие к крупным проблемам, требующим скорейшего решения:

* использование несогласованных методов обеспечения информационной безопасности для разных компонентов сети, включая телекоммуникационные протоколы, информационные ресурсы и приложения;
* широкое использование технических средств импортного производства, потенциально имеющих не декларированные возможности ("закладки");
* отсутствие комплексных решений по обеспечению информационной безопасности при интеграции и взаимодействии сетей;
* недостаточная проработка методологии документирования функционирования сетей, необходимого для создания доказательной базы правонарушений;
* широко распространённое отношение к обеспечению информационной безопасности как к товару или услуге, которые можно купить, а не как к процессу, который нужно не только создать, но который нужно внедрить в постоянное использование и которым необходимо постоянно управлять.

Наиболее часто встречающиеся дефекты защиты, отмеченные компаниями, работающими в области электронного бизнеса и защиты информации:

* общие проблемы в брандмауэрах, операционных системах, сетях и стандартных приложениях;
* неопознанные машины или приложения в сети;
* использование старых версий программного обеспечения на машинах сети;
* неполная информация обо всех точках входа в сеть из внешней среды;
* неполное изъятие прав доступа при увольнении сотрудников, наличие идентификаторов пользователей, используемых по умолчанию, неверно обслуживаемые права доступа;
* неоправданно открытые порты в брандмауэрах;
* необоснованный общий доступ к файловым системам;
* недостаточные требования к идентификации пользователя, собирающегося изменить регистрационные записи пользователей;
* присутствие ненужных сервисов или приложений на машинах, требующих высокой степени защиты;
* использование слабозащищенных установочных параметров, присваиваемых по умолчанию при инсталляции приложений, ввиду чего становятся известны идентификаторы и пароли пользователей, установленные по умолчанию;
* отсутствие защиты от взаимодействия внутреннего и внешнего трафика сети;
* отсутствие проверок после внесения изменений в среду (например, после инсталляции новых приложений или машин);
* отсутствие контроля вносимых изменений;
* отсутствие информации о внутренних угрозах безопасности;
* отсутствие информации о слабых местах различных методик аутентификации при организации мощной защиты.

Любая успешная *атака* нарушителя, направленная на реализацию угрозы информационной безопасности сети, опирается на полученные нарушителем знания об особенностях её построения и слабых местах. Причинами появления уязвимостей в сетях могут быть:

* уязвимые зоны в поставляемом программном продукте;
* нарушение технологий передачи информации и управления;
* внедрение компонентов и программ, реализующих не декларированные функции и нарушающих нормальное функционирование сетей;
* невыполнение реализованными механизмами защиты сети заданных требований к процессу обеспечения информационной безопасности или предъявление непродуманного набора требований;
* использование не сертифицированных в соответствии с требованиями безопасности отечественных и зарубежных информационных технологий, средств информатизации и связи, а также средств защиты информации и контроля их эффективности.

Постоянный *аудит* сетей связи с целью выявления уязвимостей и возможных угроз обеспечивает *определение* "слабого звена", а уровень защищённости "слабого звена" определяет, в конечном счёте, уровень информационной безопасности сети в целом.

Принципиальным является рассмотрение воздействий нарушителей или атак как неизбежного фактора функционирования сетей и систем связи. Это обстоятельство является обратной стороной информатизации экономики и бизнеса.

В этих условиях обеспечение информационной безопасности сетей становится триединой задачей, включающей *мониторинг* функционирования, обнаружение атак и принятие адекватных мер противодействия.

Адекватные меры противодействия могут носить технический характер и предусматривать реконфигурацию информационной области сети. Они могут быть также организационными и предусматривать обращение операторов сетей связи к силовым структурам с предоставлением необходимой информации для выявления и привлечения к ответственности нарушителей.

Обеспечение информационной безопасности сетей, систем и средств связи означает *создание процесса*, которым необходимо постоянно управлять и который является неотъемлемой составной частью процесса функционирования компьютерных вычислительных устройств и сетей. Построив модель функционирования сети, включающую *процесс управления* обеспечением информационной безопасности, необходимо далее определить стандарты информационной безопасности, поддерживающие эту модель. *Значение* исследований процессов стандартизации и совершенствования нормативно-правовой базы будут постоянно возрастать.

Вопросы информационной безопасности, защиты информации и данных неразрывно связаны с безопасностью программно-аппаратных комплексов и сетевых устройств, образующих *информационные системы* и сети различного назначения. Такие системы должны отвечать серьёзным требованиям по обеспечению надёжности сбора, обработки, архивирования и передачи данных по открытым и закрытым сетям и обеспечению их максимальной защиты.

**Определение защищенной информационной системы**

В отличие от локальных корпоративных сетей, подключенных к Internet, где обычные средства безопасности в большой степени решают проблемы защиты внутренних сегментов сети от несанкционированного доступа, распределенные корпоративные информационные системы, системы электронной коммерции и предоставления услуг пользователям Internet предъявляют повышенные требования в плане обеспечения информационной безопасности.

Межсетевые экраны, системы обнаружения атак, сканеры для выявления уязвимостей в узлах сети, операционных систем и СУБД, фильтры пакетов данных на маршрутизаторах — достаточно ли всего этого мощного арсенала (так называемого "жёсткого периметра") для обеспечения безопасности критически важных информационных систем, работающих в Internet и Intranet? Практика и накопленный к настоящему времени опыт показывают — чаще всего нет!

В "Оранжевой книге" надежная и защищённая информационная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную достоверную обработку информации разной степени секретности различными пользователями или группами пользователей без нарушения прав доступа, целостности и конфиденциальности данных и информации, и поддерживающая свою работоспособность в условиях воздействия на неё совокупности внешних и внутренних угроз" [Department of Defense Trusted Computer System Evaliation Criteria (TCSEC). USA DoD 5200.28-STD, 1993] .

Это качественное определение содержит необходимое и достаточное условие безопасности. При этом не обуславливается, какие механизмы и каким образом реализуют безопасность — практическая реализация зависит от многих факторов: вида и размера бизнеса, предметной области деятельности компании, типа информационной системы, степени её распределённости и сложности, топологии сетей, используемого программного обеспечения и т.д.

Концепция "Защищенные информационные системы" включает ряд законодательных инициатив, научных, технических и технологических решений, готовность государственных организаций и компаний использовать их для того, чтобы люди, используя устройства на базе компьютеров и программного обеспечения, чувствовали себя так же комфортно и безопасно. В общем случае можно говорить о степени доверия, или надежности систем, оцениваемых по двум основным критериям: наличие и полнота политики безопасности и гарантированность безопасности.

Наличие и полнота политики безопасности — набор внешних и корпоративных стандартов, правил и норм поведения, отвечающих законодательным актам страны и определяющих, как организация собирает, обрабатывает, распространяет и защищает информацию. В частности, стандарты и правила определяют, в каких случаях и каким образом пользователь имеет право оперировать с определенными наборами данных. В политике безопасности сформулированы права и ответственности пользователей и персонала. В зависимости от сформулированной политики можно выбирать конкретные механизмы, обеспечивающие безопасность системы. Чем больше информационная система и чем больше она имеет "входов" и "выходов" (распределённая система), тем "строже", детализированнее и многообразнее должна быть политика безопасности.

Гарантированность безопасности — мера доверия, которая может быть оказана архитектуре, инфраструктуре, программно-аппаратной реализации системы и методам управления её конфигурацией и целостностью. Гарантированность может проистекать как из тестирования и верификации, так и из проверки (системной или эксплуатационной) общего замысла и исполнения системы в целом и ее компонентов. Гарантированность показывает, насколько корректны механизмы, отвечающие за проведение в жизнь политики безопасности. Гарантированность является пассивным, но очень важным компонентом защиты, реализованным качеством разработки, внедрения, эксплуатации и сопровождения информационной системы и заложенных принципов безопасности.

Концепция гарантированности является центральной при оценке степени, с которой информационную систему можно считать надежной. Надежность определяется всей совокупностью защитных механизмов системы в целом и надежностью вычислительной базы (ядра системы), отвечающих за проведение в жизнь политики безопасности. Надежность вычислительной базы определяется ее реализацией и корректностью исходных данных, вводимых административным и операционным персоналом. Оценка уровня защищенности ИТ/ИС обычно производится по трём базовым группам критериев ([табл. 1](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27503?page=1#table.1)).

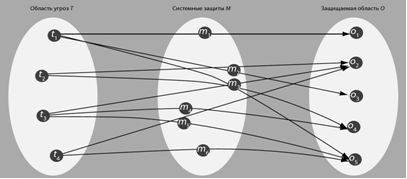
|  |  |  |
| --- | --- | --- |
| Таблица 1. Трёхуровневая модель параметров оценки защищенности ИС | | |
| **Система целей** | **Средства** | **Исполнение** |
| Общая цель   * Защищенные информационные системы   Цели   * Безопасность * Безотказность * Надежность * Деловое взаимодействие | Обеспечение   * Защищенность * Конфиденциальность * Целостность * Готовность к работе * Точность * Управляемость * Безотказность * Прозрачность * Удобство пользования   Подтверждение доверия   * Внутренняя оценка * Аккредитация * Внешний аудит | Установки   * Законы, нормы * Характер ведения бизнеса * Контракты, обязательства * Внутренние принципы * Международные, отраслевые, и внутренние стандарты   Реализация   * Методы взаимодействия с внешней и внутренней средой * Методы работ * Анализ рисков * Методы разработки, внедрения, эксплуатации и сопровождения * Обучение персонала |

Основное назначение надежной вычислительной базы — выполнять функции монитора обращений и действий, то есть контролировать допустимость выполнения пользователями определенных операций над объектами. Монитор проверяет каждое обращение к программам или данным на предмет их согласованности со списком допустимых действий. Таким образом, важным средством обеспечения безопасности является механизм подотчетности или протоколирования. Надежная система должна фиксировать все события, касающиеся безопасности, а ведение протоколов дополняется аудитом — анализом регистрационной информации.

Эти общие положения являются основой для проектирования и реализации безопасности открытых информационных систем [Зегжда Д.П., Ивашко А.М., 2000].

**Методология анализа защищенности информационной системы**

При разработке архитектуры и создании инфраструктуры корпоративной ИС неизбежно встает вопрос о её защищенности от угроз. Решение вопроса состоит в подробном анализе таких взаимно пересекающихся видов работ, как реализация ИС и её аттестация, аудит и обследование безопасности ИС [Астахов А.Н., 2002].

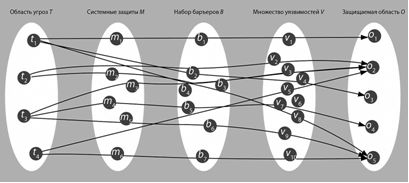


**Рис. 5.1.**Модель системы защиты с полным перекрытием

Основой формального описания систем защиты традиционно считается модель системы защиты с полным перекрытием ([рис. 5.1](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27503?page=2#image.5.1)), в которой рассматривается взаимодействие "области угроз", "защищаемой области" и "системы защиты". Таким образом, имеем три множества: T = {_ti} — множество угроз безопасности, O = {o_j} — множество объектов (ресурсов) защищенной системы, M = {m_k} — множество механизмов безопасности АС.

Элементы этих множеств находятся между собой в определенных отношениях, собственно и описывающих систему защиты. Для описания системы защиты обычно используется графовая модель. Множество отношений угроза-объект образует двухдольный граф {T, O}. Цель защиты состоит в том, чтобы перекрыть все возможные ребра в графе. Это достигается введением третьего набора M; в результате получается трехдольный граф {T, M, O}.

Развитие модели предполагает введение еще двух элементов ([рис. 5.2](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27503?page=2#image.5.2)). Здесь V — набор уязвимых мест, определяемый подмножеством декартова произведения {T*O}: v_r = <t_i, o_j>. Под уязвимостью системы защиты понимают возможность осуществления угрозы T в отношении объекта O. (На практике под уязвимостью системы защиты обычно понимают, те свойства системы, которые либо способствуют успешному осуществлению угрозы, либо могут быть использованы злоумышленником для её осуществления).



**Рис. 5.2.**Модель системы защиты, содержащей уязвимости

Определим B как набор барьеров, определяемый декартовым произведением {V*M}: b_l = <t_i, o_j, m_k>, представляющих собой пути осуществления угроз безопасности, перекрытые средствами защиты. В результате получаем систему, состоящую из пяти элементов: <T, O, M, V, B>, описывающую систему защиты с учетом наличия уязвимостей.

Для системы с полным перекрытием для любой уязвимости имеется устраняющий ее барьер. Иными словами, в подобной системе защиты для всех возможных угроз безопасности существуют механизмы защиты, препятствующие осуществлению этих угроз. Данное условие является первым фактором, определяющим защищенность ИС, второй фактор — "прочность" и надёжность механизмов защиты.

В идеале каждый механизм защиты должен исключать соответствующий путь реализации угрозы. В действительности же механизмы защиты обеспечивают лишь определённую степень сопротивляемости угрозам безопасности. Поэтому в качестве характеристик элемента набора барьеров b_l = <t_i, o_j, m_k> может рассматриваться набор <P_l, L_l, R_l>, где P_l — вероятность появления угрозы, L_l — величина ущерба при удачном осуществлении угрозы в отношении защищаемых объектов (уровень серьезности угрозы), а R_l — степень сопротивляемости механизма защиты m_k, характеризующаяся вероятностью его преодоления.

Надёжность барьера b_l = <t_i, o_j, m_k> характеризуется величиной остаточного риска Risk_l, связанного с возможностью осуществления угрозы t_i в отношении объекта информационной системы o_j при использовании механизма защиты mk. Эта величина определяется по формуле: Risk_l = P_k*L_k*(1– R_k). Для нахождения примерной величины защищенности S можно использовать следующую простую формулу: S= 1/Risk_0, где Risk_0 является суммой всех остаточных рисков, (0<[P_k , L_k ]<1), ( 0 \le R_k<1 ).

Суммарная величина остаточных рисков характеризует приблизительную совокупную уязвимость системы защиты, а защищенность определяется как величина, обратная уязвимости. При отсутствии в системе барьеров b_k, "перекрывающих" выявленные уязвимости, степень сопротивляемости механизма защиты R_k принимается равной нулю.

На практике получение точных значений приведенных характеристик барьеров затруднено, поскольку понятия угрозы, ущерба и сопротивляемости механизма защиты трудно формализовать. Так, оценку ущерба в результате несанкционированного доступа к информации политического и военного характера точно определить вообще невозможно, а определение вероятности осуществления угрозы не может базироваться на статистическом анализе. Построение моделей системы защиты и анализ их свойств составляют предмет "теории безопасных систем", еще только оформляющейся в качестве самостоятельного направления.

Вместе с тем, для защиты информации экономического характера, допускающей оценку ущерба, разработаны стоимостные методы оценки эффективности средств защиты. Для этих методов набор характеристик барьера дополняет величина C_l затраты на построение средства защиты барьера b_l. В этом случае выбор оптимального набора средств защиты связан с минимизацией суммарных затрат W={w_l}, состоящих из затрат C={c_l} на создание средств защиты и возможных затрат в результате успешного осуществления угроз N={n_l}.

Формальные подходы к решению задачи оценки защищенности из-за трудностей, связанных с формализацией, широкого практического распространения не получили. Значительно более действенным является использование неформальных классификационных подходов. Для этого применяют категорирование: нарушителей (по целям, квалификации и доступным вычислительным ресурсам); информации (по уровням критичности и конфиденциальности); средств защиты (по функциональности и гарантированности реализуемых возможностей), эффективности и рентабельности средств защиты и т. п.