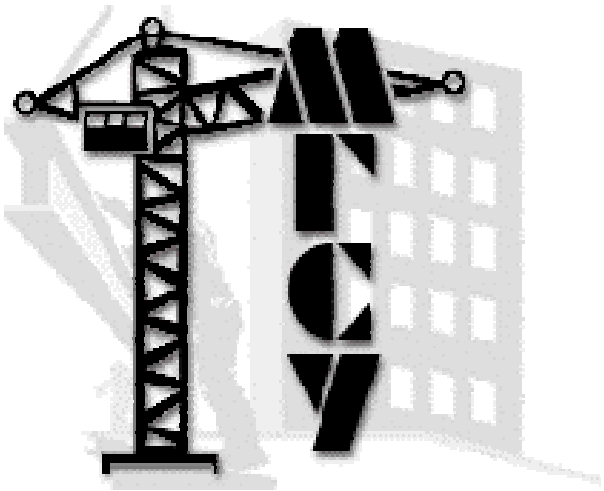
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ
кафедра “САПР в строительстве”

проф., к.т.н. Гаряев Н.А.

Курс лекций

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



Москва 2005 г.

Содержание

Лекция 1. Введение.

Информационная безопасность - это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации - это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности - это оборотная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

- Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты. В первом случае "пусть лучше все сломается, чем враг узнает хоть один секретный бит", во втором - " нет у нас никаких секретов, лишь бы все работало".
- Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственно защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте.

Возвращаясь к вопросам терминологии, отметим, что термин "компьютерная безопасность" (как эквивалент или заменитель ИБ) представляется нам слишком узким. ***Компьютеры - только одна из составляющих информационных систем***, и хотя наше внимание будет сосредоточено в первую очередь на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее безопасность определяется всей совокупностью составляющих и, в первую очередь, самым слабым звеном, которым в подавляющем большинстве случаев оказывается человек (записавший, например, свой пароль на "горчичнике", прилепленном к монитору).

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Эта инфраструктура имеет самостоятельную ценность, но нас будет интересовать лишь то, как она влияет на выполнение информационной системой предписанных ей функций.

Обратим внимание, что в определении ИБ перед существительным "ущерб" стоит прилагательное "неприемлемый". Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда ***стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба***. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а **целью защиты информации становится уменьшение размеров ущерба до допустимых значений**.

Основные виды и источники атак на информацию

Современное состояние информационной безопасности

Атака на информацию – это умышленное нарушение правил работы с информацией. Атаки на информацию могут принести предприятию огромные убытки. На сегодняшний день примерно 90% всех атак на информацию производят ныне работающие либо уволенные с предприятия сотрудники.

Последнее время сообщения об атаках на информацию, о хакерах и компьютерных взломах наполнили все средства массовой информации. Что же такое "атака на информацию"? Дать определение этому действию на самом деле очень сложно, поскольку информация, особенно в электронном виде, представлена сотнями различных видов. Информацией можно считать и отдельный файл, и базу данных, и одну запись в ней, и целиком программный комплекс. И все эти объекты могут подвергнуться и подвергаются атакам со стороны некоторой социальной группы лиц.

При хранении, поддержании и предоставлении доступа к любому информационному объекту его владелец, либо уполномоченное им лицо, накладывает набор правил по работе с ней. **Умышленное их нарушение классифицируется как атака на информацию.**

С массовым внедрением компьютеров во все сферы деятельности человека объем информации, хранимой в электронном виде вырос в тысячи раз. И теперь скопировать за полминуты и унести дискету с файлом, содержащим план выпуска продукции, намного проще, чем копировать или пе-

реписывать кипу бумаг. А с появлением компьютерных сетей даже отсутствие физического доступа к компьютеру перестало быть гарантией сохранности информации.

Каковы возможные последствия атак на информацию? В первую очередь, конечно, нас будут интересовать экономические потери:

1. Раскрытие коммерческой информации может привести к серьезным прямым убыткам на рынке
2. Известие о краже большого объема информации обычно серьезно влияет на репутацию фирмы, приводя косвенно к потерям в объемах торговых операций
3. Фирмы-конкуренты могут воспользоваться кражей информации, если та осталась незамеченной, для того чтобы полностью разорить фирму, навязывая ей фиктивные либо заведомо убыточные сделки
4. Подмена информации как на этапе передачи, так и на этапе хранения в фирме может привести к огромным убыткам
5. Многократные успешные атаки на фирму, предоставляющую какой-либо вид информационных услуг, снижают доверие к фирме у клиентов, что сказывается на объеме доходов

Естественно, компьютерные атаки могут принести и огромный моральный ущерб. Понятие конфиденциального общения давно уже стало "притчей во языцех". Само собой разумеется, что никакому пользователю компьютерной сети не хочется, чтобы его письма кроме адресата получали еще 5-10 человек, или, например, весь текст, набираемый на клавиатуре ЭВМ, копировался в буфер, а затем при подключении к Интернету отправлялся на определенный сервер. А именно так и происходит в тысячах и десятках тысяч случаев.

Несколько интересных цифр об атаках на информацию. Они были получены исследовательским центром DataPro Research в 1998 году. Основные причины повреждений электронной информации распределились следующим образом: неумышленная ошибка человека – 52% случаев, умышленные действия человека - 10% случаев, отказ техники – 10% случаев, повреждения в результате пожара - 15% случаев, повреждения водой – 10% случаев. Как видим, каждый десятый случай повреждения электронных данных связан с компьютерными атаками.

Кто был исполнителем этих действий: в 84% случаев – текущий кадровый состав учреждений, только в 10% случаев – совершенно посторонние люди, и в 6% случаев – бывшие работники этих же учреждений. Доля атак, производимых сотрудниками фирм и предприятий, просто ошеломляет и заставляет вспомнить не только о технических, но и о психологических методах профилактики подобных действий.

И, наконец, что же именно предпринимают злоумышленники, добравшись до информации: в 44% случаев взлома были произведены непосредственные кражи денег с электронных счетов, в 16% случаев выводилось из строя программное обеспечение, столь же часто – в 16% случаев – производилась кража информации с различными последствиями, в 12% случаев информация была сфальсифицирована, в 10% случаев злоумышленники с помощью компьютера воспользовались либо заказали услуги, к которым в принципе не должны были иметь доступа.

Категории информационной безопасности

В тех случаях, когда идет речь о безопасности, в отношении информации и информационно-вычислительных систем применяются общепринятые термины о свойствах этих объектов – категории.

Информация с точки зрения информационной безопасности обладает следующими категориями:

- **конфиденциальность** – гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется хищением либо раскрытием информации
- **целостность** – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения
- **аутентичность** – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется фальсификацией, но уже автора сообщения
- **апеллируемость** – довольно сложная категория, но часто применяемая в электронной коммерции – гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой; отличие этой категории от предыдущей в том, что при подмене автора, кто-то другой пытается заявить, что он автор сообщения, а при нарушении апеллируемости – сам автор пытается "откреститься" от своих слов, подписанных им однажды.

В отношении информационных систем применяются иные категории:

- **надежность** – гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано
- **точность** – гарантия точного и полного выполнения всех команд
- **контроль доступа** – гарантия того, что различные группы лиц имеют различный доступ к информационным объектам, и эти ограничения доступа постоянно выполняются

- **контролируемость** – гарантия того, что в любой момент может быть произведена полноценная проверка любого компонента программного комплекса
- **контроль идентификации** – гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает
- **устойчивость к умышленным сбоям** – гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как оговорено заранее.

Обзор наиболее распространенных методов "взлома"

Часто злоумышленники проникают в систему не напрямую, "сражаясь" с системами шифрования или идентификации, а "в обход", используя либо явные промахи создателей, не заметивших какой-либо очень простой метод обойти их систему, либо ошибки в реализации программ защиты. Также злоумышленники широко используют психологические приемы для того, чтобы получить нужную им информацию у рядовых сотрудников фирм.

Комплексный поиск возможных методов доступа

Злоумышленники очень тщательно изучают системы безопасности перед проникновением в нее. Очень часто они находят очевидные и очень простые методы "взлома" системы, которые создатели просто "проглядели", создавая возможно очень хорошую систему идентификации или шифрования.

Обратимся к наиболее популярным и очевидным технологиям несанкционированного доступа. Рассматривая их мы должны использовать очень простое правило: **"прочность цепи не выше прочности самого слабого ее звена".** Эта аксиома постоянно цитируется, когда речь идет о компьютерной безопасности. Например, как бы ни была прочна система, если пароль на доступ к ней лежит в текстовом файле в центральном каталоге или записан на экране монитора – это уже не конфиденциальная система. А примеров, в которых разработчики системы защиты забывают или просто не учитывают какие-либо примитивнейшие методы проникновения в систему, можно найти сотни, и мы будем с ними сталкиваться в ходе нашего курса.

Например, при работе в сети Internet не существует надежного автоматического подтверждения того, что данный пакет пришел именно от того отправителя (IP-адреса), который заявлен в пакете. А это позволяет даже при применении самого надежного метода идентификации первого пакета подменять все остальные, просто заявляя, что все они пришли тоже с этого же самого IP-адреса.

Примерно та же проблема существует в сети Novell NetWare 3.11 – в ней сервер может поддерживать одновременно до 254 станций, и при этом при наличии мощной системы идентификации аутентификация пакета ведется только по номеру станции. Это позволяло проводить следующую атаку – в присутствии в сети клиента-супервизора злоумышленнику достаточно послать 254 пакета с командой серверу, которую он хочет исполнить, перебрав в качестве псевдо-отправителя все 254 станции. Один из отправленных пакетов совпадет с номером соединения, на котором сейчас действительно находится клиент-супервизор, и команда будет принята сервером к исполнению, а остальные 253 пакета просто проигнорированы.

А в отношении шифрования – мощного средства защиты передаваемой информации от прослушивания и изменения – можно привести следующий метод, неоднократно использованный на практике. Действительно злоумышленник, не зная пароля, которым зашифрованы данные или команды, передаваемые по сети, не может прочесть их или изменить. Но если у него есть возможность наблюдать, что происходит в системе после получения конкретного блока данных (например, стирается определенный файл или выключается какое-либо аппаратное устройство), то он может, не раскодируя информацию, послать ее повторно и добьется результатов, аналогичных команде супервизора.

Все это заставляет разработчиков защищенных систем постоянно помнить и о самых простых и очевидных способах проникновения в систему и предупреждать их в комплексе.

Терминалы защищенной информационной системы

Терминалы – это точки входа пользователя в информационную сеть. В том случае, когда к ним имеют доступ несколько человек или вообще любой желающий, при их проектировании и эксплуатации необходимо тщательное соблюдение целого комплекса мер безопасности.

Несмотря на самоочевидность, все-таки **наиболее распространенным** способом входа в систему при атаках на информацию остается вход через официальный log-in запрос системы. Вычислительная техника, которая позволяет произвести вход в систему, называется в теории информационной безопасности терминалом. Терминология восходит к временам суперЭВМ и тонких "терминальных" клиентов. Если система состоит всего из одного персонального компьютера, то он одновременно считается и терминалом и сервером. Доступ к терминалу может быть физическим, в том случае, когда терминал – это ЭВМ с клавиатурой и дисплеем, либо удаленным – чаще всего по интернет каналам.

При использовании терминалов с физическим доступом необходимо соблюдать следующие требования:

1. Защищенность терминала должна соответствовать защищенности помещения: терминалы без пароля могут присутствовать только в тех помещениях, куда имеют доступ лица соответствующего или более высокого уровня доступа. **Отсутствие имени регистрации возможно только в**

том случае, если к терминалу имеет доступ только один человек, либо если на группу лиц, имеющих к нему доступ, распространяются общие меры ответственности. Терминалы, установленные в публичных местах должны всегда запрашивать имя регистрации и пароль.

2. Системы контроля за доступом в помещение с установленным терминалом должны работать полноценно и в соответствии с общей схемой доступа к информации.
3. В случае установки терминала в местах с широким скоплением народа клавиатура, а если необходимо, то и дисплей должны быть оборудованы устройствами, позволяющими видеть их только работающему в данный момент клиенту (непрозрачные стеклянные или пластмассовые ограждения, шторки, "утопленная" модель клавиатуры).

При использовании удаленных терминалов необходимо соблюдать следующие правила:

1. Любой удаленный терминал должен запрашивать имя регистрации и пароль. Того, что якобы никто не знает IP и пароля вашего компьютера, отнюдь не достаточно для конфиденциальности вашей системы. Все дело в том, что при наличии программного обеспечения, которое не составит труда найти в сети Интернет, за несколько минут можно перебрать около миллиона паролей доступа к вашему компьютеру. И подобные операции производятся довольно часто, особенно в отношении фирм, связанных с компьютерами и компьютерными сетями, а также в отношении промышленных предприятий.
2. Вторым требованием является своевременное отключение всех терминалов, не требующихся в данный момент фирме (например, по вечерам, либо во время обеденного перерыва), либо не контролируемых в данный момент Вашими сотрудниками.
3. Из log-in запроса терминала рекомендуется убрать все непосредственные упоминания имени фирмы, ее логотипы и т.п. – это не позволит компьютерным вандалам, просто перебирающим номера с IP, узнать log-in экран какой фирмы они обнаружили. Для проверки правильности соединения вместо имени фирмы можно использовать неординарную приветственную фразу, какой-либо афоризм либо просто фиксированную последовательность букв и цифр, которые будут запоминаться у постоянных операторов этого терминала.
4. Также на входе в систему рекомендуется выводить на экран предупреждение о том, что вход в систему без полномочий на это преследуется по закону. Во-первых, это послужит еще одним предостережением начинающим злоумышленникам, а во-вторых, будет надежным аргументом в пользу атакованной фирмы в судебном разбирательстве, если таковое будет производиться.

Безотносительно от физического или коммутируемого доступа к терминалу, линия, соединяющая терминал (коммутируемый, либо установленный в публичном месте) с зоной ядра информационной системы должна быть защищена от прослушивания, либо же весь обмен информацией должен вестись по конфиденциальной схеме идентификации и надежной схеме аутентификации клиента – этим занимаются криптосистемы.

Получение пароля на основе ошибок администратора и пользователей

Дальнейшие действия взломщика, получившего доступ к терминальной точке входа, могут развиваться по двум основным направлениям:

а) попытки выяснения пароля прямо или косвенно;

Перебор паролей по словарю являлся некоторое время одной из самых распространенных техник подбора паролей. В настоящее время, как хоть самый малый результат пропаганды информационной безопасности, он стал сдавать свои позиции. Хотя развитие быстродействия вычислительной техники и все более сложные алгоритмы составления слов-паролей не дают "погибнуть" этому методу. Технология перебора паролей родилась в то время, когда самым сложным паролем было скажем слово "brilliant", а в русифицированных ЭВМ оно же, но для "хитрости" набранное в латинском режиме, но глядя на русские буквы (эта тактика к сожалению до сих пор чрезвычайно распространена, хотя и увеличивает информационную насыщенность пароля всего на 1 бит). В то время простенькая программа со словарем в 5000 существительных давала положительный результат в 90% случаев. Огромное число инцидентов со взломами систем заставило пользователей добавлять к словам 1-2 цифры с конца, записывать первую и/или последнюю букву в верхнем регистре, но это увеличило время на перебор вариантов с учетом роста быстродействия ЭВМ всего в несколько раз. Так в 1998 году было официально заявлено, что даже составление двух совершенно не связанных осмысленных слов подряд, не дает сколь либо реальной надежности паролю. К этому же времени получили широкое распространение языки составления паролей, записывающие в абстрактной форме основные принципы составления паролей среднестатистическими пользователями ЭВМ.

Следующей модификацией подбора паролей является проверка паролей, устанавливаемых в системах по умолчанию. В некоторых случаях администратор программного обеспечения, проинсталлировав или получив новый продукт от разработчика, не удосуживается проверить, из чего состоит система безопасности. Как следствие, пароль, установленный в фирме разработчике по умолчанию, остается основным паролем в системе. ***В сети Интернет можно найти огромные списки паролей по умолчанию практически ко всем версиям программного обеспечения, если они устанавливаются на нем производителем.***

Основные требования к информационной безопасности, основанные на анализе данного метода, следующие:

- Вход всех пользователей в систему должен подтверждаться вводом уникального для клиента пароля.
- ***Пароль должен тщательно подбираться так, чтобы его информационная емкость соответствовала времени полного перебора пароля.*** Для этого необходимо детально инструктировать клиентов о понятии "простой к подбору пароль", либо передать операцию выбора пароля в ведение инженера по безопасности.
- ***Пароли по умолчанию должны быть сменены*** до официального запуска системы и даже до сколь либо публичных испытаний программного комплекса. Особенно это относится к сетевому программному обеспечению.

1. Все ошибочные попытки войти в систему должны учитываться, записываться в файл журнала событий и анализироваться через "разумный" промежуток времени. Если в системе предусмотрена возможность блокирования клиента либо всей системы после определенного количества неудачных попыток входа, этой возможностью необходимо воспользоваться. Если же Вы являетесь разработчиком системы безопасности, данную возможность несомненно необходимо предусмотреть, так как она является основным барьером к подбору паролей полным перебором. Разумно блокировать клиента после 3-ей подряд неправильной попытки набора пароля, и, соответственно, блокировать систему после K=max(int(N*0.1*3)+1 , 3) неудачных попыток входа за некоторый период (час, смену, сутки). В данной формуле N – среднее количество подключающихся за этот период к системе клиентов, 0.1 – 10%-ный предел "забывчивости пароля", 3 – те же самые три попытки на вспоминание пароля. Естественно, информация о блокировании клиента или системы должна автоматически поступать на пульт контроля за системой.
2. В момент отправки пакета подтверждения или отвержения пароля в системе должна быть установлена разумная задержка (2-5 секунд). Это не позволит злоумышленнику, попав на линию с хорошей связью до объекта атаки перебирать по сотне тысяч паролей за секунду.
3. *Все действительные в системе пароли желательно проверять современными программами подбора паролей, либо оценивать лично администратору системы.*
4. *Через определенные промежутки времени необходима принудительная смена пароля у клиентов.* Наиболее часто используемыми интервалами смены пароля являются год, месяц и неделя (в зависимости от уровня конфиденциальности информации и частоты входа в систему).
5. *Все неиспользуемые в течение долгого времени имена регистрации должны переводиться в закрытое* (недоступное для регистрации) состояние. Это относится к сотрудникам, находящимся в отпуске, на больничном, в командировке, а также к именам регистрации, созданным для тестов, испытаний системы и т.п.
6. От сотрудников и всех операторов терминала необходимо требовать строгое неразглашение паролей, отсутствие каких-либо взаимосвязей пароля с широкоизвестными фактами и данными, и отсутствие бумажных записей пароля "из-за плохой памяти".

Получение пароля на основе ошибок в реализации

б) попытки входа в систему совершенно без знания пароля, основываясь на ошибках в реализации программного или аппаратного обеспечения.

Следующей по частоте использования является методика получения паролей из самой системы. Однако, здесь уже нет возможности дать какие-либо общие рекомендации, поскольку все методы атаки зависят только от программной и аппаратной реализации конкретной системы. Основными двумя возможностями выяснения пароля являются несанкционированный доступ к носителю, содержащему их, либо использование недокументированных возможностей и ошибок в реализации системы.

Первая группа методов основана на том, что любой системе приходится где-либо хранить подлинники паролей всех клиентов для того, чтобы сверять их в момент регистрации. При этом пароли могут храниться как в открытом текстовом виде, как это имеет место во многих клонах UNIX, так и представленные в виде малозначащих контрольных сумм (хеш-значений), как это реализовано в ОС Windows, Novell NetWare и многих других. Проблема в том, что в данном случае для хранения паролей на носителе не может быть использована основная методика защиты – шифрование. Действительно, если все пароли зашифрованы каким-либо ключом, то этот ключ тоже должен храниться в самой системе для того, чтобы она работала автоматически, не спрашивая каждый раз у администратора разрешение "Пускать или не пускать пользователя Anton, Larisa, Victor и т.д.?". Поэтому, получив доступ к подобной информации, злоумышленник может либо восстановить пароль в читабельном виде (что бывает довольно часто), либо отправлять запросы, подтвержденные данным хеш-значением, не раскодируя его. Все рекомендации по предотвращению хищений паролей состоят в проверке не доступен ли файл с паролями, либо таблица в базе данных, хранящая эти пароли, кому-либо еще кроме администраторов системы, не создается ли системой резервных файлов, в местах доступных другим пользователям и т.п. . В принципе, поскольку кража паролей является самым грубым вторжением в систему, разработчики уделяют ей довольно пристальное внимание, и соблюдения всех рекомендаций по использованию системы обычно достаточно для предотвращения подобных ситуаций.

Получение доступа к паролям благодаря недокументированным возможностям систем встречается в настоящее время крайне редко. Ранее эта методика использовалась разработчиками намного чаще в основном в целях отладки, либо для экстренного восстановления работоспособности системы. Но постепенно с развитием как технологий обратной компиляции, так и информационной связанности мира она постепенно стала исчезать. Любые недокументированные возможности рано или поздно становятся известными, после чего новость об этом с головокружительной быстротой облетает мир и разработчикам приходится рассылать всем пользователям скомпрометированной системы "программные заплатки" либо новые версии программного продукта. Единственной мерой профилактики данного метода является постоянный поиск на серверах, посвященных компьютерной безопасности, объявлений обо всех неприятностях с программным обеспечением, установленным в Вашем учреждении. Для разработчиков же необходимо помнить, что любая подобная встроенная возможность может на порядок снизить общую безопасность системы, как бы хорошо она не была завуалирована в коде программного продукта.

Следующей распространенной технологией получения паролей является копирование буфера клавиатуры в момент набора пароля на терминале. Этот метод используется редко, так для него необходим доступ к терминальной машине с возможностью запуска программ. Но если злоумышленник все-таки получает подобный доступ, действенность данного метода очень высока:

1. Работа программы-перехватчика паролей (так называемого "троянского коня") на рабочей станции незаметна.
2. Подобная программа сама может отправлять результаты работы на заранее заданные сервера или анонимным пользователям, что резко упрощает саму процедуру получения паролей хакером, и затрудняет поиск и доказательство его вины. У нас в России, например, широкое распространение получила подобная троянская программа, подписывающаяся к самораспаковывающимся архивам.

Двумя основными методами борьбы с копированием паролей являются:

1).адекватная защита рабочих станций от запуска сторонних программ:

а) отключение сменных носителей информации (гибких дисков),

б) специальные драйвера, блокирующие запуск исполнимых файлов без ведома оператора, либо администратора,

в) мониторы, уведомляющие о любых изменениях системных настроек и списка автоматически запускаемых программ,

2).очень мощная, но неудобная мера – система единовременных паролей (при каждой регистрации в системе клиентам с очень высоким уровнем ответственности самой системой генерируется новый пароль).

Сканирование современными антивирусными программами также может помочь в обнаружении "троянских" программ, но только тех из них, которые получили широкое распространение по стране. А следовательно, программы, написанные злоумышленниками специально для атаки на Вашу систему, будут пропущены антивирусными программами без каких-либо сигналов.

Следующий метод получения паролей относится только к сетевому программному обеспечению. Проблема заключается в том, что во многих программах не учитывается возможность перехвата любой информации, идущей по сети – так называемого сетевого трафика. Первоначально, с внедрением локальных компьютерных сетей так оно и было. Сеть располагалась в пределах 2-3 кабинетов, либо здания с ограниченным физическим доступом к кабелям. Однако, стремительное развитие глобальных сетей затребовало на общий рынок те же версии программного обеспечения без какого-либо промедления для усиления безопасности. Теперь мы пожинаем плоды этой тенденции. Более половины протоколов сети Интернет передают пароли в нешифрованном виде – открытым текстом. К ним относятся протоколы передачи электронной почты SMTP и POP3, протокол передачи файлов FTP, одна из схем авторизации на WWW-серверах.

Современное аппаратное и программное обеспечение позволяет получать всю информацию, проходящую по сегменту сети, к которому подключен конкретный компьютер, и анализировать ее в реальном масштабе времени. Возможны несколько вариантов прослушивания трафика: 1) это может сделать служащий компании со своего рабочего компьютера, 2) злоумышленник, подключившийся к сегменту с помощью портативной ЭВМ или более мобильного устройства. Наконец, трафик, идущий от Вас к Вашему партнеру или в другой офис по сети Интернет, технически может прослушиваться со стороны Вашего непосредственного провайдера, со стороны любой организации, предоставляющей транспортные услуги для сети Интернет (переписка внутри страны в среднем идет через 3-4 компании, за пределы страны – через 5-8). Кроме того, если в должной мере будет реализовываться план СОРМ (система оперативно-розыскных мероприятий в компьютерных сетях), то возможно прослушивание и со стороны силовых ведомств страны.

Для комплексной защиты от подобной возможности кражи паролей необходимо выполнять следующие меры:

1. Физический доступ к сетевым кабелям должен соответствовать уровню доступа к информации.
2. При определении топологии сети следует при любых возможностях избегать широковещательных топологий. Оптимальной единицей сегментирования является группа операторов с равными правами доступа, либо если эта группа составляет более 10 человек, то комната или отдел внутри группы. **Ни в коем случае на одном кабеле не должны находиться операторы с разными уровнями доступа, если только весь передаваемый трафик не шифруется, а идентификация не производится по скрытой схеме без открытой передачи пароля.**
3. Ко всем информационным потокам, выходящим за пределы фирмы, должны применяться те же правила, что и только что описанные выше для объединения разноуровневых терминалов.

Социальная психология и иные способы получения паролей

Иногда злоумышленники вступают и в прямой контакт с лицами, обладающими нужной им информацией, разыгрывая довольно убедительные сцены. "Жертва" обмана, поверившая в реальность рассказанной ей по телефону или в электронном письме ситуации, сама сообщает пароль злоумышленнику.

Краткий обзор еще нескольких довольно часто встречающихся методов.

Звонок администратору – злоумышленник выбирает из списка сотрудников того, кто не использовал пароль для входа в течение нескольких дней (отпуск, отгулы, командировка) и кого администратор не знает по голосу. Затем следует звонок с объяснением ситуации о забытом пароле, искренние извинения, просьба зачитать пароль, либо сменить его на новый. Больше чем в половине случаев просьба будет удовлетворена, а факт подмены будет замечен либо с первой неудачной попыткой зарегистрироваться истинного сотрудника, либо по произведенному злоумышленником ущербу.

Почти такая же схема, но в обратную сторону может быть разыграна злоумышленником в адрес сотрудника фирмы – **звонок от администратора.** В этом случае он представляется уже сотрудником службы информационной безопасности и просит назвать пароль либо из-за произошедшего сбоя в базе данных, либо якобы для подтверждения личности самого сотрудника по какой-либо причине (рассылка особо важных новостей), либо по поводу последнего подключения сотрудника к какому-либо информационному серверу внутри фирмы. Фантазия в этом случае может придумывать самые правдоподобные причины, по которым сотруднику "просто необходимо" вслух назвать пароль. Самое неприятное в этой схеме то, что если причина запроса пароля придумана, что называется "с умом", то сотрудник повторно позвонит в службу информационной безопасности только через неделю, месяц, если вообще это произойдет. Кроме того, данная схема может быть проведена и без телефонного звонка – по электронной почте, что неоднократно и исполнялось якобы от имени почтовых и Web-серверов в сети Интернет.

Оба данных метода относятся к группе "атака по социальной психологии" и могут принимать самые разные формы. Их профилактикой может быть только тщательное разъяснение всем сотрудникам, в особо важных случаях введение административных мер и особого регламента запроса и смены пароля.

Необходимо тщательно инструктировать сотрудников об опасности оставления рабочих станций, не закрытых паролем. В первую очередь это, конечно, относится к терминалам, работающим в публичных местах и офисах с более низким уровнем доступа к информации, однако, и при работе в помещениях с равным уровнем доступа не рекомендуется давать возможность сотрудникам работать за другими ЭВМ тем более в отсутствие владельца. **В качестве программных профилактических мер используются экранные заставки с паролем, появляющиеся через 5-10 минут отсутствия рабочей активности, автоматическое отключение сервером клиента через такой же промежуток времени. От сотрудников должны требоваться разрегистрация, как на серверах, так и на рабочих станциях при выключении ЭВМ, либо закрытие их паролем при оставлении без присмотра.**

Большое внимание следует уделять любым носителям информации, покидающим пределы фирмы. Наиболее частыми причинами этого бывают ремонт аппаратуры и списание технологически устаревшей техники. Необходимо помнить, что на рабочих поверхностях носителей даже в удаленных областях находится информация, которая может представлять либо непосредственный интерес, либо косвенно послужить причиной вторжения в систему. Так, например, при использовании виртуальной памяти часть содержимого ОЗУ записывается на жесткий диск, что теоретически может привезти даже к сохранению пароля на постоянном носителе (хотя это и маловероятно). Ремонт, производимый сторонними фирмами на месте, должен производится под контролем инженера из службы информационной безопасности. Необходимо помнить, что при нынешнем быстродействии ЭВМ копирование файлов производится со скоростью, превышающей мегабайт в секунду, а установить второй жесткий диск для копирования в момент ремонта без надзора специалиста можно практически незаметно. Все носители информации, покидающие фирму должны надежно чиститься либо уничтожаться механически (в зависимости от дальнейших целей их использования).

Немного слов о защищенности самих носителей информации. На сегодняшний день не существует разумных по критерию "цена/надежность" носителей информации, не доступных к взлому. Строение файлов, их заголовки и расположение в любой операционной системе может быть прочитано при использовании соответствующего программного обеспечения. Практически невскрываемым может быть только энергонезависимый носитель, автоматически разрушающий информацию при попытке несанкционированного подключения к любым точкам, кроме разрешенных разъемов,

желательно саморазрушающийся при разгерметизации, имеющий внутри микропроцессор, анализирующий пароль по схеме без открытой передачи. Однако, все это из области "сумасшедших" цен и военных технологий.

Для бизнес-класса и частной переписки данная проблема решается гораздо проще и дешевле – с помощью криптографии. Любой объем информации от байта до гигабайта, будучи зашифрован с помощью более или менее стойкой криптосистемы, недоступен для прочтения без знания ключа. И уже совершенно не важно, хранится он на жестком диске, на дискете или компакт-диске, не важно под управлением какой операционной системы. Против самых новейших технологий и миллионных расходов здесь стоит математика, и этот барьер до сих пор невозможно преодолеть. Вот почему силовые ведомства практически всех стран, будучи не в состоянии противостоять законам математики, применяют административные меры против так называемой стойкой криптографии". Вот почему ее использование частными и юридическими лицами без лицензии Федерального Агентства по Связи и Информации (ФАПСИ), входящего в структуру одного из силовых ведомств государства, запрещено и у нас в России.

Лекция 2. Наиболее распространенные угрозы

Основные определения и критерии классификации угроз

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку, - злоумышленником. Потенциальные злоумышленники называются источниками угрозы.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, **называется окном опасности**, *ассоциированным с данным уязвимым местом.* Пока существует окно опасности, возможны успешные атаки на ИС.

Если речь идет об ошибках в ПО, то окно опасности "открывается" с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда - недель), поскольку за это время должны произойти следующие события:

- должно стать известно о средствах использования пробела в защите;
- должны быть выпущены соответствующие заплаты;
- заплаты должны быть установлены в защищаемой ИС.

Мы уже указывали, что новые уязвимые места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда существуют окна опасности и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат - как можно более оперативно.

Отметим, что некоторые угрозы нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Рассмотрим наиболее распространенные угрозы, которым подвержены современные информационные системы. **Иметь представление о возможных угрозах, а также об уязвимых местах, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности. Слишком много мифов существует в сфере информационных технологий (вспомним все ту же "Проблему 2000"), поэтому незнание в данном случае ведет к перерасходу средств и, что еще хуже, к концентрации ресурсов там, где они не особенно нужны, за счет ослабления действительно уязвимых направлений.**

Само понятие "угроза" в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать - вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Мы попытаемся взглянуть на предмет с точки зрения типичной (на наш взгляд) организации. Впрочем, многие угрозы (например, пожар) опасны для всех.

Угрозы можно классифицировать по нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

В качестве основного критерия мы будем использовать первый (по аспекту ИБ), привлекая при необходимости остальные.

Наиболее распространенные угрозы доступности

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь - следствие непреднамеренных ошибок.

Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе.

Очевидно, **самый радикальный способ борьбы с непреднамеренными ошибками - максимальная автоматизация и строгий контроль.**

Другие угрозы доступности классифицируем по компонентам ИС, на которые нацелены угрозы:

- отказ пользователей;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

- нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.)

Основными источниками внутренних отказов являются:

- отступление (случайное или умышленное) от установленных правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
- ошибки при (пере)конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Весьма опасны так называемые **"обиженные" сотрудники** - нынешние и бывшие. Как правило, они стремятся нанести вред организации-"обидчику", например:

- испортить оборудование;
- встроить логическую бомбу, которая со временем разрушит программы и/или данные;
- удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Опасны, разумеется, стихийные бедствия и события, воспринимаемые как стихийные бедствия,- пожары, наводнения, землетрясения, ураганы. По статистике, на долю огня, воды и тому подобных "злоумышленников" (среди которых самый опасный - перебой электропитания) приходится 13% потерь, нанесенных информационным системам.

Некоторые примеры угроз доступности

Угрозы доступности могут выглядеть грубо - как повреждение или даже разрушение оборудования (в том числе носителей данных). Такое повреждение может вызываться естественными причинами (чаще всего - грозами). К сожалению, находящиеся в массовом использовании источники бесперебойного питания не защищают от мощных кратковременных импульсов, и случаи выгорания оборудования - не редкость.

В принципе, мощный кратковременный импульс, способный разрушить данные на магнитных носителях, можно сгенерировать и искусственным образом - с помощью так называемых высокоэнергетических радиочастотных пушек. Но, наверное, в наших условиях подобную угрозу следует все же признать надуманной.

Действительно опасны протечки водопровода и отопительной системы. Часто организации, чтобы сэкономить на арендной плате, снимают помещения в домах старой постройки, делают косметический ремонт, но не меняют ветхие трубы.

Летом, в сильную жару, ломаются кондиционеры, установленные в серверных залах, набитых дорогостоящим оборудованием. В результате значительный ущерб наносится и репутации, и кошельку организации.

Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если это предложение выполняется, резервные носители зачастую хранят небрежно, не обеспечивая их защиту от вредного воздействия окружающей среды. И когда требуется восстановить данные, оказывается, что эти самые носители никак не желают читаться.

Перейдем теперь к угрозам доступности, которые будут похитрее засоров канализации. Речь пойдет о программных атаках на доступность.

В качестве средства вывода системы из штатного режима эксплуатации может использоваться агрессивное потребление ресурсов (обычно - полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти). По расположению источника угрозы такое потребление подразделяется на локальное и удаленное. При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Простейший пример удаленного потребления ресурсов - атака, получившая наименование "SYN-наводнение". Она представляет собой попытку переполнить таблицу "полуоткрытых" TCP-соединений сервера (установление соединений начинается, но не заканчивается). Такая атака по меньшей мере затрудняет установление новых соединений со стороны легальных пользователей, то есть сервер выглядит как недоступный.

По отношению к атаке "Papa Smurf" уязвимы сети, воспринимающие ping-пакеты с широковещательными адресами. Ответы на такие пакеты "съедают" полосу пропускания.

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме - как скоординированные распределенные атаки, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание. Временем начала "моды" на подобные атаки можно считать февраль 2000 года, когда жертвами оказались несколько крупнейших систем электронной коммерции (точнее - владельцы и пользователи систем). Отметим, что если имеет место архитектурный просчет в виде разбалансированности между пропускной способностью сети и производительностью сервера, то защититься от распределенных атак на доступность крайне трудно.

Для выведения систем из штатного режима эксплуатации могут использоваться уязвимые места в виде программных и аппаратных ошибок. Например, известная ошибка в процессоре Pentium I дает возможность локальному пользователю путем выполнения определенной команды "подвесить" компьютер, так что помогает только аппаратный RESET.

Программа "Teardrop" удаленно "подвешивает" компьютеры, эксплуатируя ошибку в сборке фрагментированных IP-пакетов.

Вредоносное программное обеспечение

Одним из опаснейших способов проведения атак является внедрение в атакуемые системы вредоносного программного обеспечения.

Мы выделим следующие грани вредоносного ПО:

- вредоносная функция;
- способ распространения;
- внешнее представление.

Часть, осуществляющую разрушительную функцию, будем называть "**бомбой**" (хотя, возможно, более удачными терминами были бы "заряд" или "боеголовка"). Вообще говоря, спектр вредоносных функций неограничен, поскольку **"бомба",** как и любая другая программа, может обладать сколь угодно сложной логикой, но обычно "бомбы" предназначаются для:

- внедрения другого вредоносного ПО;
- получения контроля над атакуемой системой;
- агрессивного потребления ресурсов;
- изменения или разрушения программ и/или данных.

По механизму распространения различают:

- вирусы - код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;
- "черви" - код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы).

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. "Черви", напротив, ориентированы в первую очередь на путешествия по сети.

Иногда само распространение вредоносного ПО вызывает агрессивное потребление ресурсов и, следовательно, является вредоносной функцией. Например, "черви" "съедают" полосу пропускания сети и ресурсы почтовых систем. По этой причине для атак на доступность они не нуждаются во встраивании специальных "бомб".

Вредоносный код, который выглядит как функционально полезная программа, называется троянским. Например, обычная программа, будучи пораженной вирусом, становится троянской; порой троянские программы изготавливают вручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке.

Отметим, что данные нами определения и приведенная классификация вредоносного ПО отличаются от общепринятых. Например, в ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения" содержится следующее определение:

"**Программный вирус** - это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах".

Окно опасности для вредоносного ПО появляется с выпуском новой разновидности "бомб", вирусов и/или "червей" и перестает существовать с обновлением базы данных антивирусных программ и наложением других необходимых заплат.

По традиции из всего вредоносного ПО наибольшее внимание общественности приходится на долю вирусов. Однако до марта 1999 года с полным правом можно было утверждать, что "несмотря на экспоненциальный рост числа известных вирусов, аналогичного роста количества инцидентов, вызванных ими, не зарегистрировано. **Соблюдение несложных правил "компьютерной гигиены" практически сводит риск заражения к нулю.** Там, где работают, а не играют, число зараженных компьютеров составляет лишь доли процента".

В марте 1999 года, с появлением вируса "Melissa", ситуация кардинальным образом изменилась. "Melissa" - это макровирус для файлов MS-Word, распространяющийся посредством электронной почты в присоединенных файлах. Когда такой (зараженный) присоединенный файл открывают, он рассылает свои копии по первым 50 адресам из адресной книги Microsoft Outlook. В результате почтовые серверы подвергаются атаке на доступность.

В данном случае нам хотелось бы отметить два момента.

1. Как уже говорилось, пассивные объекты отходят в прошлое; так называемое активное содержимое становится нормой. Файлы, которые по всем признакам должны были бы относиться к данным (например, документы в форматах MS-Word или Postscript, тексты почтовых сообщений), способны содержать интерпретируемые компоненты, которые могут запускаться неявным образом при открытии файла. Как и всякое в целом прогрессивное явление, такое "повышение активности данных" имеет свою оборотную сторону (в рассматриваемом случае - отставание в разработке механизмов безопасности и ошибки в их реализации). Обычные пользователи еще не скоро научатся применять интерпретируемые компоненты "в мирных целях" (или хотя бы узнают об их существовании), а перед злоумышленниками открылось по существу неограниченное поле деятельности. Как ни банально это звучит, но если для стрельбы по воробьям выкатывается пушка, то пострадает в основном стреляющий.
2. Интеграция разных сервисов, наличие среди них сетевых, всеобщая связность многократно увеличивают потенциал для атак на доступность, облегчают распространение вредоносного ПО (вирус "Melissa" - классический тому пример). Образно говоря, многие информационные системы, если не принять защитных мер, оказываются "в одной лодке" (точнее - в корабле без переборок), так что достаточно одной пробоины, чтобы "лодка" тут же пошла ко дну.

Как это часто бывает, вслед за "Melissa" появилась на свет целая серия вирусов, "червей" и их комбинаций: "Explorer.zip" (июнь 1999), "Bubble Boy" (ноябрь 1999), "ILOVEYOU" (май 2000) и т.д. *Не то что бы от них был особенно большой ущерб, но общественный резонанс они вызвали немалый.*

Активное содержимое, помимо интерпретируемых компонентов документов и других файлов данных, имеет еще одно популярное обличье - так называемые мобильные агенты. Это программы, которые загружаются на другие компьютеры и там выполняются. Наиболее известные примеры мобильных агентов - Java-апплеты, загружаемые на пользовательский компьютер и интерпретируемые Internet-навигаторами. Оказалось, что разработать для них модель безопасности, оставляющую достаточно возможностей для полезных действий, не так-то просто; еще сложнее реализовать такую модель без ошибок. В августе 1999 года стали известны недочеты в реализации технологий ActiveX и Java в рамках Microsoft Internet Explorer, которые давали возможность размещать на Web-серверах вредоносные апплеты, позволяющие получать полный контроль над системой-визитером.

Для внедрения "бомб" часто используются ошибки типа "переполнение буфера", когда программа, работая с областью памяти, выходит за границы допустимого и записывает в нужные злоумышленнику места определенные данные. Так действовал еще в 1988 году знаменитый "червь Моррриса"; в июне 1999 года хакеры нашли способ использовать аналогичный метод по отношению к Microsoft Internet Information Server (IIS), чтобы получить контроль над Web-сервером. Окно опасности охватило сразу около полутора миллионов серверных систем...

Не забыты современными злоумышленниками и испытанные троянские программы. Например, "троянцы" Back Orifice и Netbus позволяют получить контроль над пользовательскими системами с различными вариантами MS-Windows.

Таким образом, действие вредоносного ПО может быть направлено не только против доступности, но и против других основных аспектов информационной безопасности.

Основные угрозы целостности.

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги. По данным газеты USA Today, еще в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий ущерб в размере 882 миллионов долларов. Можно предположить, что реальный ущерб был намного больше, поскольку многие организации по понятным причинам скрывают такие инциденты; не вызывает сомнений, что в наши дни ущерб от такого рода действий вырос многократно.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз, хотя говорят и пишут о них значительно меньше, чем о внешних.

Ранее мы проводили различие между статической и динамической целостностью. С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

- ввести неверные данные;
- изменить данные.

Иногда изменяются содержательные данные, иногда - служебная информация. Показательный случай нарушения целостности имел место в 1996 году. Служащая Oracle (личный секретарь вице-президента) предъявила судебный иск, обвиняя президента корпорации в незаконном увольнении после того, как она отвергла его ухаживания. В доказательство своей правоты женщина привела электронное письмо, якобы отправленное ее начальником президенту. Содержание письма для нас сейчас не важно; важно время отправки. Дело в том, что вице-президент предъявил, в свою очередь, файл с регистрационной информацией компании сотовой связи, из которого явствовало, что в указанное время он разговаривал по мобильному телефону, находясь вдалеке от своего рабочего места. Таким образом, в суде состоялось противостояние "файл против файла". Очевидно, один из них был фальсифицирован или изменен, то есть была нарушена его целостность. Суд решил, что подделали электронное письмо (секретарша знала пароль вице-президента, поскольку ей было поручено его менять), и иск был отвергнут...

(Теоретически возможно, что оба фигурировавших на суде файла были подлинными, корректными с точки зрения целостности, а письмо отправили пакетными средствами, однако, на наш взгляд, это было бы очень странное для вице-президента действие.)

Из приведенного случая можно сделать вывод не только об угрозах нарушения целостности, но и об опасности слепого доверия компьютерной информации. Заголовки электронного письма могут быть подделаны; письмо в целом может быть фальсифицировано лицом, знающим пароль отправителя (мы приводили соответствующие примеры). Отметим, что последнее возможно даже тогда, когда целостность контролируется криптографическими средствами. Здесь имеет место взаимодействие разных аспектов информационной безопасности: если нарушена конфиденциальность, может пострадать целостность.

Еще один урок: угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить "неотказуемость", компьютерные данные не могут рассматриваться в качестве доказательства.

Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и программы. Внедрение рассмотренного выше вредоносного ПО - пример подобного нарушения.

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

Выводы. Основные угрозы конфиденциальности

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе, а то и попросту теряет. И дело здесь не в неорганизованности людей, а в изначальной непригодности парольной схемы. Невозможно помнить много разных паролей; рекомендации по их регулярной (по возможности - частой) смене только усугубляют положение, заставляя применять несложные схемы чередования или вообще стараться свести дело к двум-трем легко запоминаемым (и столь же легко угадываемым) паролям.

Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена (зачастую - и не может быть обеспечена) необходимая защита. Угроза же состоит в том, что кто-то не откажется узнать секреты, которые сами просятся в руки. Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным перехват данных. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п.), но идея одна - осуществить доступ к данным в тот момент, когда они наименее защищены.

Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании ИС, но и, что очень важно, при всех изменениях. Весьма опасной угрозой являются... выставки, на которые многие организации, недолго думая, отправляют оборудование из производственной сети, со всеми хранящимися на них данными. Остаются прежними пароли, при удаленном доступе они продолжают передаваться в открытом виде. Это плохо даже в пределах защищенной сети организации; в объединенной сети выставки - это слишком суровое испытание честности всех участников.

Еще один пример изменения, о котором часто забывают, - хранение данных на резервных носителях. Для защиты данных на основных носителях применяются развитые системы управления доступом; копии же нередко просто лежат в шкафах и получить доступ к ним могут многие.

Перехват данных - очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например на кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных. Часто ноутбуки оставляют без присмотра на работе или в автомобиле, иногда просто теряют.

Опасной нетехнической угрозой конфиденциальности являются методы морально-психологического воздействия, такие как маскарад - выполнение действий под видом лица, обладающего полномочиями для доступа к данным (см., например, статью Айрэ Винклера "Задание: шпионаж" в Jet Info, 1996, 19).

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример - нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Таковы основные угрозы, которые наносят наибольший ущерб субъектам информационных отношений.

Внутренний спам – информационная атака.

Борьба со спамом в последнее время стала едва ли не единственным вопросом, волнующим Интернет-сообщество. Как грибы после дождя, появляются сайты, посвященные методам такой борьбы, выпускаются бесплатные фильтры спама. Средства массовой информации насаждают "спамофобию", публикуя оценки грядущих объемов спама и материального вреда, который он причиняет.

Оправдывая прогноз директора исследований группы Giga Джонатана Пенна, рынок антиспамерских программ быстро развивается. На одном только сайте SecurityLab.ru можно скачать порядка 20 бесплатных программ, реализующих те или иные механизмы борьбы с этим явлением. Делаются попытки объявить спам вне закона.

Кому нужен СПАМ?

Как показывает практика, борьба со спамом проходит без особого успеха. И так будет до тех пор, пока объектом этой борьбы будет следствие, а не причина. А причина спама заключается в том, что это - экономически эффективное средство маркетинга, несмотря на крайне низкий процент откликов на него. Ведь его эффективность рассчитывается не по абсолютному числу откликов, а по

соотношению результата к затратам. А затраты на массовые рассылки минимальны. Следовательно, спам эффективен при любом результате!

Нижеследующие данные приводятся не в первый раз, но они весьма показательны

	Рассылка по традиционной почте	Рассылка по электронной почте
Затраты на 1 письмо	$0,25	$0,0008
Ожидаемый отклик	0,03%	0,000025%
Затраты на отклик	$12	$0,032

т.е. эффективность рассылки по электронной почте в 375 раз выше.

Спам - вчерашний день?

Недавние исследования, проведенные компанией eMarketer, показали, что эффективность e-mail-рекламы снижается. "Причина - в человеческой психологии, - говорит ведущий аналитик eMarketer Дэвид Холлерман. - Пресыщаясь броскими лозунгами, которые переполняют электронные почтовые ящики, люди попросту перестают обращать на них внимание".

Остается надеяться, что невнимание к непрошеным письмам когда-нибудь сделает этот вид рекламы менее рентабельным. По прогнозам компании Brightmail, в 2004 году количество спама, на который сегодня приходится свыше половины электронной почты, начнет уменьшаться и к 2005-2006 году снизится до 10%, а может даже 5% почтового трафика.

Однако есть несколько категорий товаров, которые, пользуясь определенным спросом, могут распространяться только таким образом. Как ни странно, это именно та самая "Виагра", пиратские DVD, интимный досуг и тому подобные услуги и продукция.

Есть еще один аргумент в пользу спама: он дает возможность продвигать торговые марки. Заметьте, что когда к вам приходит предложение приобрести в фирме Х товары ИЗВЕСТНОЙ МАРКИ, то все негативные эмоции (которые, кстати, имеют тенденцию забываться) направлены в адрес фирмы Х. Предложение товаров ИЗВЕСТНОЙ МАРКИ, попавшие на плодородную почву (как, например, кондиционер в жаркий день), могут заинтересовать получателя письма.

Кроме того, на смену традиционному спаму идет технология "Вирус", которая подразумевает рассылку писем от знакомых к знакомым. С учетом того, что каждый человек имеет в среднем до 100 знакомых, с которыми он ведет переписку по электронной почте, скорость распространения писем при этом представляется достаточно высокой. Правда, большую роль в этой технологии играет содержание и оформление письма.

Спам и закон

Единственным законом, регулирующим вопросы спама в нашей стране, как ни странно, является Конституция. Некоторые спамеры дают ссылку на 4-ю часть 29-й статьи Конституции РФ, в которой сказано, что каждый имеет право свободно искать, получать, **передавать, производить и распространять информацию** любым законным способом (Весьма забавно видеть такую ссылку, вставленную в письмо с предложением услуг бригады маляров). Получается, что спамер не нарушает никаких законов.

Восполнить этот пробел решил Российский комитет Программы ЮНЕСКО. Он начал разработку проекта Федерального закона "О несанкционированной рассылке электронных сообщений" и пригласил всех желающих поучаствовать в проекте "Антиспам".

Трудности с написанием закона начались сразу - на этапе формулирования основных определений. Вот, например, как вводится в этом проекте понятие "Несанкционированная рассылка (НР) электронного сообщения" (Авторские права © Российский комитет Программы ЮНЕСКО "Информация для всех"):

"Рассылка электронного сообщения является несанкционированной, если:

- сообщение было послано в адрес неопределенного круга лиц, или
- получатель сообщения изъявлял ранее нежелание получать сообщения от лица, производящего рассылку, или от лица, являющегося заказчиком рассылки, или
- адрес, на который было послано сообщение, получен лицом, производящим рассылку, или лицом, являющимся заказчиком рассылки, незаконно.

Массовая рассылка - рассылка, одного и того же сообщения или идентичных по содержанию сообщений по двум и более адресам во временном промежутке, не превышающем 24 часа".

Получается, вроде бы, похоже на описание спама. Но определение это допускает слишком широкое толкование, ибо под него можно подвести практически любую переписку, в том числе и личную: откуда можно узнать, желает ли конкретный адресат получать это конкретное сообщение? А одинарная массовая рассылка вообще может не попасть под это определение.

Явно, что до принятия конкретных мер в масштабах государства еще далеко, так что спасение утопающих в море спама - дело рук самих утопающих…

Но так ли страшен черт, как его малюют?

Существует предположение, что спамеры напрасно тратят время на написание писем и деньги на трафик, поскольку их рассылки уже никто не читает. Исследование, проведенное сайтом silicon.com, показало, что более 90% непрошеных писем отравляются в корзину сразу после получения.

В любом случае, как показывает практика, спам - это, скорее, проблема конечного, домашнего пользователя. Что касается корпоративного пользователя, то тут проблема переходит в несколько иную плоскость.

Некоммерческая организация Pew Internet and American Life Project опубликовала интересное исследование об использовании электронной почты в американском корпоративном секторе. Как оказалось, такая острая проблема, как спам, не слишком актуальна для лиц, пользующихся электронной почтой на работе, и потерь рабочего времени из-за переполнения ящика назойливой рекламой практически не возникает.

Объем электронной корреспонденции на работе для большинства американцев невелик. 60% из них получают не более десяти писем за день, 23% владельцев рабочих почтовых ящиков получают от 20 до 50 писем в день, и только 6% имеют дело более чем с 50 письмами за сутки.

Существует много оценок того ущерба, который спам наносит корпоративным пользователям. Вот пример одного из них:

По разным оценкам, более **30% входящего почтового трафика организаций составляет спам.** При среднем размере письма в 20 кбайт и получении каждым сотрудником примерно 50 сообщений в день совершенно излишний трафик организации, где электронную почту получают 100 человек, превышает 6,8 Гбайт за год, что при стоимости трафика в $30 за гигабайт составляет $204 в год.

Если предположить, что "забитость" ненужной информацией почтовых ящиков не самое страшное, то, наверное, **основной ущерб от спама вызван падением производительности труда: сотрудники вынуждены отвлекаться на спам**. Оказалось, что каждый сотрудник тратит в среднем 4,5 секунды на удаление одного такого письма.

Продолжим расчет: 15 писем по 5 секунд - чуть больше 1 минуты в день! Из месячного оклада в $500 на удаление спама теряется примерно $1,5, что в расчете на 100 пользователей дает $150 в месяц и $1800 в год.

Итого, компания из 100 человек из-за спама теряет минимум $2000 в год.

"Корпоративный" спам

Гораздо больший урон работодателю наносят его же сотрудники.

По данным той же Pew Internet and American Life Project, 75% служащих признались, что используют Интернет на работе в личных целях, 39% опрошенных рассылают по почте юмор, 26% обсуждают свою личную жизнь, а 15% - сплетничают.

И если даже сотрудник тратит на чтение заинтересовавшего его спамового письма минуту (которая, напомню, при зарплате в 500$ стоит работодателю около 5 центов), то на чтение "25 причин, почему пиво лучше, чем женщина" уйдет гораздо больше времени.

Кроме того, подобный текст транслируется всем знакомым в компании и за ее пределами (не напоминает технологию "Вирус"?). Да и сами эти материалы не возникают из воздуха: они приходят через ту же корпоративную электронную почту или выискиваются самими сотрудниками через Интернет (но это уже отдельная тема). А Вы не сталкивались с ситуацией, когда, разослав "Анекдот дня" по 10 адресам своей адресной книги Вы сами получаете его от 11-го адресата? А если предположить, что в такую ситуацию попадают многие?

Но и это еще не все. Десятки "лучших анекдотов" распечатываются для чтения в транспорте по пути на работу. В курилке обсуждаются лучшие остроты и раздаются обещания переслать ссылки на них. Более того, многие пользователи пересылают своим знакомым развлекательные картинки и видеоролики.

Ущерб от подобных действий можно примерно оценить. Если сотрудники тратят на все вышеописанное час своего времени в день, то каждый из них зря получает ежемесячно около 60 долларов, а организация со штатом в 100 человек соответственно теряет $6000 в месяц. За год это составляет порядка $70 тыс. оплаченного за счет работодателя досуга сотрудников.

Но не все люди имеют одинаковое понятие о том, что можно считать смешным. То, что в понятии одного человека является шуткой, может оскорбить другого. Такие шутки, свободно циркулирующие во внутренней почтовой системе, могут представлять угрозу для организации: случайно отправленные не по назначению (например, клиенту), они могут стать причиной разрыва отношений или даже судебного преследования.

Методы защиты

Защита от "корпоративного" спама существует. Имя ей - средства контроля содержимого. Опасность этого вида спама в полной мере осознали на Западе: свои решения в этой сфере сегодня предлагают такие именитые компании как Symantec и Clearswift. Последняя, по данным компании IDS, со своим флагманским продуктом MIMEsweeper является лидером на этом новом для России рынке.

Принцип работы фильтров содержимого электронной почты и Интернет-трафика основан на указании разрешенных и запрещенных адресов электронной почты, IP-адресов хостов, замеченных в рассылке спама, а также на поиске определенных слов в передаваемых текстах.

Стоимость подобных фильтрующих систем составляет несколько тысяч долларов, что позволяет им для компании, несущей вышеупомянутые убытки в $70 тыс. в год, окупаться в течение одного месяца, при том, что они способны решать одновременно ряд других задач, таких как антивирусная защита, а также контроль исходящей почты на предмет утечки конфиденциальных материалов.

Выводы

Итак, как нам удалось выяснить, спам можно разделить на две большие категории:

- обычный, который у многих ассоциируется с "Центром американского английского" и наносит ущерб в основном тем, кто пользуется бесплатными почтовыми ящиками,
- "корпоративный", представляющий собой почтовый обмен сотрудников между собой и со своими знакомыми.

Для того чтобы ответить на вопрос, какого спама опасаться и как от него защищаться, надо еще раз вспомнить о том, что "спасение утопающих в море спама - дело рук самих утопающих…".

Лекция 3. Законодательный уровень информационной безопасности

Что такое законодательный уровень информационной безопасности и почему он важен

В деле обеспечения информационной безопасности успех может принести только **комплексный подход**. Мы уже указывали, что для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательного;
- административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- процедурного (меры безопасности, ориентированные на людей);
- программно-технического.

Законодательный уровень является важнейшим для обеспечения информационной безопасности. **Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.**

Мы будем различать на законодательном уровне две группы мер:

- меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (назовем их мерами ограничительной направленности);
- направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

На практике обе группы мер важны в равной степени, но хотелось бы выделить аспект осознанного соблюдения норм и правил ИБ. Это важно для всех субъектов информационных отношений, поскольку рассчитывать только на защиту силами правоохранительных органов было бы наивно. Необходимо это и тем, в чьи обязанности входит наказывать нарушителей, поскольку обеспечить доказательность при расследовании и судебном разбирательстве компьютерных преступлений без специальной подготовки невозможно.

Самое важное (и, вероятно, самое трудное) на законодательном уровне - создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

Обзор российского законодательства в области информационной безопасности. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 - право на знание достоверной информации о состоянии окружающей среды.

В принципе, **право на информацию** может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

Статья 23 Конституции гарантирует **право на личную и семейную тайну**, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 - право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к **средствам защиты информации.**

В Гражданском кодексе Российской Федерации (в своем изложении мы опираемся на редакцию от 15 мая 2001 года) фигурируют такие понятия, как **банковская, коммерческая и служебная тайна.** Согласно статье 139, информация составляет **служебную или коммерческую тайну** в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Это подразумевает, как минимум, компетентность в вопросах ИБ и наличие доступных (и законных) средств обеспечения конфиденциальности.

Весьма продвинутым в плане информационной безопасности является Уголовный кодекс Российской Федерации (редакция от 14 марта 2002 года). Глава 28 - "Преступления в сфере компьютерной информации" - содержит три статьи:

- статья 272. Неправомерный доступ к компьютерной информации;
- статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
- статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Первая имеет дело с посягательствами на конфиденциальность, вторая - с вредоносным ПО, третья - с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ. Включение в сферу действия УК РФ вопросов доступности информационных сервисов представляется нам очень своевременным.

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе **"О государственной тайне"** (с изменениями и дополнениями от 6 октября 1997 года). В нем гостайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средств защиты информации. Согласно данному Закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации. Подчеркнем важность последней части определения.

Закон "Об информации, информатизации и защите информации"

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информатизации и защите информации" от 20 февраля 1995 года номер 24-ФЗ (принят Государственной Думой 25 января 1995 года). В нем даются основные определения и намечаются направления развития законодательства в данной области.

Процитируем некоторые из этих определений:

- информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- документированная информация (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
- информационные процессы - процессы сбора, обработки, накопления, хранения, поиска и распространения информации;
- информационная система - организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;
- информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
- информация о гражданах (персональные данные) - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
- конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;
- пользователь (потребитель) информации - субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Мы, разумеется, не будем обсуждать качество данных в Законе определений. Обратим лишь внимание на гибкость определения конфиденциальной информации, которая не сводится к сведениям, составляющим государственную тайну, а также на понятие персональных данных, закладывающее основу защиты последних.

Закон выделяет следующие цели защиты информации:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Отметим, что Закон на первое место ставит сохранение конфиденциальности информации. Целостность представлена также достаточно полно, хотя и на втором месте. О доступности ("предотвращение несанкционированных действий по ... блокированию информации") сказано довольно мало.

Продолжим цитирование:

"Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу".

По сути, это положение констатирует, что защита информации направлена на обеспечение интересов субъектов информационных отношений.

Далее. "Режим защиты информации устанавливается:

- в отношении сведений, отнесенных к государственной тайне, - уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";
- в отношении конфиденциальной документированной информации - собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;
- в отношении персональных данных - федеральным законом."

Здесь явно выделены три вида защищаемой информации, ко второму из которых принадлежит, в частности, коммерческая информация. Поскольку защите подлежит только документированная информация, необходимым условием является фиксация коммерческой информации на материальном носителе и снабжение ее реквизитами. Отметим, что в данном месте Закона речь идет только о конфиденциальности; остальные аспекты ИБ забыты.

Обратим внимание, что защиту государственной тайны и персональных данных берет на себя государство; за другую конфиденциальную информацию отвечают ее собственники.

Как же защищать информацию? В качестве основного закон предлагает для этой цели мощные универсальные средства: **лицензирование и сертификацию**. Процитируем статью 19.

Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации "О сертификации продукции и услуг".

Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Порядок сертификации определяется законодательством Российской Федерации.

Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется законодательством Российской Федерации.

Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации.

Здесь трудно удержаться от риторического вопроса: а есть ли в России информационные системы без импортной продукции? Получается, что на защите интересов потребителей стоит в данном случае только таможня...

И еще несколько пунктов, теперь из статьи 22:

Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.

Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств. Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.

Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.

Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты информации.

Из пункта 5 следует, что должны обнаруживаться все (успешные) атаки на ИС. Вспомним в этой связи один из результатов опроса: около трети респондентов-американцев не знали, были ли взломаны их ИС за последние 12 месяцев. По нашему законодательству их можно было бы привлечь к ответственности...

Далее, статья 23 "Защита прав субъектов в сфере информационных процессов и информатизации" содержит следующий пункт:

Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба. Очень важными являются пункты статьи 5, касающиеся юридической силы электронного документа и электронной цифровой подписи:

Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью.

Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.

Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии. Порядок выдачи лицензий определяется законодательством Российской Федерации.

Таким образом, Закон предлагает действенное средство контроля целостности и решения проблемы "неотказуемости" (невозможности отказаться от собственной подписи).

Таковы важнейшие, на наш взгляд, положения Закона "Об информации, информатизации и защите информации". На следующей странице будут рассмотрены другие законы РФ в области информационной безопасности.

Другие законы и нормативные акты

Следуя логике Закона "Об информации, информатизации и защите информации", мы продолжим наш обзор Законом "О лицензировании отдельных видов деятельности" от 8 августа 2001 года номер 128-ФЗ (Принят Государственной Думой 13 июля 2001 года). Начнем с основных определений.

- **Лицензия** - специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.
- **Лицензируемый вид деятельности** - вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с настоящим Федеральным законом.
- **Лицензирование** - мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением и возобновлением действия лицензий, аннулированием лицензий и контролем лицензирующих органов за соблюдением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий.
- **Лицензирующие органы** - федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с настоящим Федеральным законом.
- **Лицензиат** - юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности."

Статья 17 Закона устанавливает перечень видов деятельности, на осуществление которых требуются лицензии. Нас будут интересовать следующие виды:

- распространение шифровальных (криптографических) средств;
- техническое обслуживание шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка и производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- выдача сертификатов ключей электронных цифровых подписей, регистрация владельцев электронных цифровых подписей, оказание услуг, связанных с использованием электронных цифровых подписей и подтверждением подлинности электронных цифровых подписей;

- выявление электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- разработка и (или) производство средств защиты конфиденциальной информации;
- техническая защита конфиденциальной информации;
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Необходимо учитывать, что, согласно статье 1, действие данного Закона не распространяется на следующие виды деятельности:

- деятельность, связанная с защитой государственной тайны;
- деятельность в области связи;
- образовательная деятельность.

Подчеркнем в этой связи, что данный Закон не препятствует организации Интернет-Университетом учебных курсов по информационной безопасности (не требует получения специальной лицензии; ранее подобная лицензия была необходима). В свою очередь, Федеральный Закон "Об образовании" не содержит каких-либо специальных положений, касающихся образовательной деятельности в области ИБ.

Основными лицензирующими органами в области защиты информации являются Федеральное агентство правительственной связи и информации (ФАПСИ) и Гостехкомиссия России. ФАПСИ ведает всем, что связано с криптографией, Гостехкомиссия лицензирует деятельность по защите конфиденциальной информации. Эти же организации возглавляют работы по сертификации средств соответствующей направленности. Кроме того, ввоз и вывоз средств криптографической защиты информации (шифровальной техники) и нормативно-технической документации к ней может осуществляться исключительно на основании лицензии Министерства внешних экономических связей Российской Федерации, выдаваемой на основании решения ФАПСИ. Все эти вопросы регламентированы соответствующими указами Президента и постановлениями Правительства РФ, которые мы здесь перечислять не будем.

В эпоху глобальных коммуникаций важную роль играет Закон "Об участии в международном информационном обмене" от 4 июля 1996 года номер 85-ФЗ (принят Государственной Думой 5 июня 1996 года). В нем, как и в Законе "Об информации...", основным защитным средством являются лицензии и сертификаты. Процитируем несколько пунктов из статьи 9.

Защита конфиденциальной информации государством распространяется только на ту деятельность по международному информационному обмену, которую осуществляют физические и юридические лица, обладающие лицензией на работу с конфиденциальной информацией и использующие сертифицированные средства международного информационного обмена.

Выдача сертификатов и лицензий возлагается на Комитет при Президенте Российской Федерации по политике информатизации, Государственную техническую комиссию при Президенте Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации. Порядок выдачи сертификатов и лицензий устанавливается Правительством Российской Федерации.

При обнаружении нештатных режимов функционирования средств международного информационного обмена, то есть возникновения ошибочных команд, а также команд, вызванных несанкционированными действиями обслуживающего персонала или иных лиц, либо ложной информацией собственник или владелец этих средств должен своевременно сообщить об этом в органы контроля за осуществлением международного информационного обмена и собственнику или владельцу взаимодействующих средств международного информационного обмена, в противном случае он несет ответственность за причиненный ущерб.

При желании здесь можно усмотреть обязательность выявления нарушителя информационной безопасности - положение, вне всяких сомнений, очень важное и прогрессивное.

Еще одна цитата - теперь из статьи 17 того же Закона.

Статья 17: "Сертификация информационных продуктов, информационных услуг, средств международного информационного обмена.

При ввозе информационных продуктов, информационных услуг в Российскую Федерацию импортер представляет сертификат, гарантирующий соответствие данных продуктов и услуг требованиям договора. В случае невозможности сертификации ввозимых на территорию Российской Федерации информационных продуктов, информационных услуг ответственность за использование данных продуктов и услуг лежит на импортере.

Средства международного информационного обмена, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих средств подлежат обязательной сертификации.

Сертификация сетей связи производится в порядке, определяемом Федеральным законом "О связи"."

Читая пункт 2, трудно удержаться от вопроса: "А нужно ли сертифицировать средства защиты средств защиты этих средств?" Ответ, конечно, положительный...

10 января 2002 года Президентом был подписан очень важный закон "Об электронной цифровой подписи" номер 1-ФЗ (принят Государственной Думой 13 декабря 2001 года), развивающий и конкретизирующий приведенные выше положения закона "Об информации...". Его роль поясняется в статье 1.

Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Закон вводит следующие основные понятия:

- **Электронный документ** - документ, в котором информация представлена в электронно-цифровой форме.
- **Электронная цифровая подпись** - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.
- **Владелец сертификата ключа подписи** - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).
- **Средства электронной цифровой подписи** - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.
- **Сертификат средств электронной цифровой подписи** - документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.
- **Закрытый ключ электронной цифровой подписи** - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.
- **Открытый ключ электронной цифровой подписи** - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.
- **Сертификат ключа подписи** - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Подтверждение подлинности электронной цифровой подписи в электронном документе - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Пользователь сертификата ключа подписи - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Информационная система общего пользования - информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Корпоративная информационная система - информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Пересказать такие определения своими словами невозможно... Обратим внимание на неоднозначное использование термина "сертификат", которое, впрочем, не должно привести к путанице. Кроме того, данное здесь определение электронного документа слабее, чем в Законе "Об информации...", поскольку нет упоминания реквизитов.

Согласно Закону, электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.
- Закон определяет сведения, которые должен содержать сертификат ключа подписи:
- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима запись об этом вносится удостоверяющим центром в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;
- наименование и местонахождение удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

Интересно, много ли Федеральных законов, содержащих такое количество технической информации и столь зависимых от конкретной технологии?

На этом мы заканчиваем обзор законов РФ, относящихся к информационной безопасности.

Обзор зарубежного законодательства в области информационной безопасности

Конечно, излишняя амбициозность заголовка очевидна. Разумеется, мы лишь пунктиром очертим некоторые законы нескольких стран (в первую очередь - США), поскольку только в США таких законодательных актов около 500.

Ключевую роль играет американский "Закон об информационной безопасности" (Computer Security Act of 1987, Public Law 100-235 (H.R. 145), January 8, 1988). Его цель - реализация минимально достаточных действий по обеспечению безопасности информации в федеральных компьютерных системах, без ограничений всего спектра возможных действий.

Характерно, что уже в начале Закона называется конкретный исполнитель - Национальный институт стандартов и технологий (НИСТ), отвечающий за выпуск стандартов и руководств, направленных на защиту от уничтожения и несанкционированного доступа к информации, а также от краж и подлогов, выполняемых с помощью компьютеров. Таким образом, имеется в виду как регламентация действий специалистов, так и повышение информированности всего общества.

Согласно Закону, все операторы федеральных ИС, содержащих конфиденциальную информацию, должны сформировать планы обеспечения ИБ. Обязательным является и периодическое обучение всего персонала таких ИС. НИСТ, в свою очередь, обязан проводить исследования природы и масштаба уязвимых мест, вырабатывать экономически оправданные меры защиты. Результаты исследований рассчитаны на применение не только в государственных системах, но и в частном секторе.

Закон обязывает НИСТ координировать свою деятельность с другими министерствами и ведомствами, включая Министерство обороны, Министерство энергетики, Агентство национальной безопасности (АНБ) и т.д., чтобы избежать дублирования и несовместимости.

Помимо регламентации дополнительных функций НИСТ, Закон предписывает создать при Министерстве торговли комиссию по информационной безопасности, которая должна:

- выявлять перспективные управленческие, технические, административные и физические меры, способствующие повышению ИБ;
- выдавать рекомендации Национальному институту стандартов и технологий, доводить их до сведения всех заинтересованных ведомств.

С практической точки зрения важен раздел 6 Закона, обязывающий все правительственные ведомства сформировать план обеспечения информационной безопасности, направленный на то, чтобы компенсировать риски и предотвратить возможный ущерб от утери, неправильного использования, несанкционированного доступа или модификации информации в федеральных системах. Копии плана направляются в НИСТ и АНБ.

В 1997 году появилось продолжение описанного закона - законопроект "О совершенствовании информационной безопасности" (Computer Security Enhancement Act of 1997, H.R. 1903), направленный на усиление роли Национального института стандартов и технологий и упрощение операций с криптосредствами.

В законопроекте констатируется, что частный сектор готов предоставить криптосредства для обеспечения конфиденциальности и целостности (в том числе аутентичности) данных, что разработка и использование шифровальных технологий должны происходить на основании требований рынка, а не распоряжений правительства. Кроме того, здесь отмечается, что за пределами США имеются сопоставимые и общедоступные криптографические технологии, и это следует учитывать при выработке экспортных ограничений, чтобы не снижать конкурентоспособность американских производителей аппаратного и программного обеспечения.

Для защиты федеральных ИС рекомендуется более широко применять технологические решения, основанные на разработках частного сектора. Кроме того, предлагается оценить возможности общедоступных зарубежных разработок.

Очень важен раздел 3, в котором от НИСТ требуется по запросам частного сектора готовить добровольные стандарты, руководства, средства и методы для инфраструктуры открытых ключей (см. выше Закон РФ об ЭЦП), позволяющие сформировать негосударственную инфраструктуру, пригодную для взаимодействия с федеральными ИС.

В разделе 4 особое внимание обращается на необходимость анализа средств и методов оценки уязвимых мест других продуктов частного сектора в области ИБ.

Приветствуется разработка правил безопасности, нейтральных по отношению к конкретным техническим решениям, использование в федеральных ИС коммерческих продуктов, участие в реализации шифровальных технологий, позволяющее в конечном итоге сформировать инфраструктуру, которую можно рассматривать как резервную для федеральных ИС.

Важно, что в соответствии с разделами 10 и далее предусматривается выделение конкретных (и немалых) сумм, называются точные сроки реализации программ партнерства и проведения исследований инфраструктуры с открытыми ключами, национальной инфраструктуры цифровых подписей. В частности, предусматривается, что для удостоверяющих центров должны быть разработаны типовые правила и процедуры, порядок лицензирования, стандарты аудита.

В 2001 году был одобрен Палатой представителей и передан в Сенат новый вариант рассмотренного законопроекта - Computer Security Enhancement Act of 2001 (H.R. 1259 RFS). В этом варианте примечательно как то, что, по сравнению с предыдущей редакцией, было убрано, так и то, что добавилось.

За четыре года (1997-2001 гг.) на законодательном и других уровнях информационной безопасности США было сделано многое. Смягчены экспортные ограничения на криптосредства (в январе 2000 г.). Сформирована инфраструктура с открытыми ключами. Разработано большое число стандартов (например, новый стандарт электронной цифровой подписи - FIPS 186-2, январь 2000 г.). Все это позволило не заострять более внимания на криптографии как таковой, а сосредоточиться на одном из ее важнейших приложений - аутентификации, рассматривая ее по отработанной на криптосредствах методике. Очевидно, что, независимо от судьбы законопроекта, в США будет сформирована национальная инфраструктура электронной аутентификации. В данном случае законотворческая деятельность идет в ногу с прогрессом информационных технологий.

Программа безопасности, предусматривающая экономически оправданные защитные меры и синхронизированная с жизненным циклом ИС, упоминается в законодательстве США неоднократно. Согласно пункту 3534 ("Обязанности федеральных ведомств") подглавы II ("Информационная безопасность") главы 35 ("Координация федеральной информационной политики") рубрики 44 ("Общественные издания и документы"), такая программа должна включать:

- периодическую оценку рисков с рассмотрением внутренних и внешних угроз целостности, конфиденциальности и доступности систем, а также данных, ассоциированных с критически важными операциями и ресурсами;
- правила и процедуры, позволяющие, опираясь на проведенный анализ рисков, экономически оправданным образом уменьшить риски до приемлемого уровня;
- обучение персонала с целью информирования о существующих рисках и об обязанностях, выполнение которых необходимо для их (рисков) нейтрализации;
- периодическую проверку и (пере)оценку эффективности правил и процедур;
- действия при внесении существенных изменений в систему;
- процедуры выявления нарушений информационной безопасности и реагирования на них; эти процедуры должны помочь уменьшить риски, избежать крупных потерь; организовать взаимодействие с правоохранительными органами.

Конечно, в законодательстве США имеются в достаточном количестве и положения ограничительной направленности, и директивы, защищающие интересы таких ведомств, как Министерство обороны, АНБ, ФБР, ЦРУ, но мы не будем на них останавливаться. Желающие могут прочитать

раздел "Законодательная база в области защиты информации" в превосходной статье О. Беззубцева и А. Ковалева "О лицензировании и сертификации в области защиты информации" (Jet Info, 1997, 4).

В законодательстве ФРГ выделим весьма развернутый (44 раздела) Закон о защите данных (Federal Data Protection Act of December 20, 1990 (BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325)). Он целиком посвящен защите персональных данных.

Как, вероятно, и во всех других законах аналогичной направленности, в данном случае устанавливается приоритет интересов национальной безопасности над сохранением тайны частной жизни. В остальном права личности защищены весьма тщательно. Например, если сотрудник фирмы обрабатывает персональные данные в интересах частных компаний, он дает подписку о неразглашении, которая действует и после перехода на другую работу.

Государственные учреждения, хранящие и обрабатывающие персональные данные, несут ответственность за нарушение тайны частной жизни "субъекта данных", как говорится в Законе. В материальном выражении ответственность ограничена верхним пределом в 250 тысяч немецких марок.

Из законодательства Великобритании упомянем семейство так называемых добровольных стандартов BS 7799, помогающих организациям на практике сформировать программы безопасности. В последующих лекциях мы еще вернемся к рассмотрению этих стандартов; здесь же отметим, что они действительно работают, несмотря на "добровольность" (или благодаря ей?).

В современном мире глобальных сетей законодательная база должна быть согласована с международной практикой. В этом плане поучителен пример Аргентины. В конце марта 1996 года компетентными органами Аргентины был арестован Хулио Цезар Ардита, 21 года, житель Буэнос-Айреса, системный оператор электронной доски объявлений "Крик", известный в компьютерном подполье под псевдонимом "El Griton". Ему вменялись в вину систематические вторжения в компьютерные системы ВМС США, НАСА, многих крупнейших американских университетов, а также в компьютерные системы Бразилии, Чили, Кореи, Мексики и Тайваня. Однако, несмотря на тесное сотрудничество компетентных органов Аргентины и США, Ардита был отпущен без официального предъявления обвинений, поскольку по аргентинскому законодательству вторжение в компьютерные системы не считается преступлением. Кроме того, в силу принципа "двойной криминальности", действующего в международных правовых отношениях, Аргентина не может выдать хакера американским властям. Дело Ардита показывает, каким может быть будущее международных компьютерных вторжений при отсутствии всеобщих или хотя бы двусторонних соглашений о борьбе с компьютерной преступностью. О текущем состоянии российского законодательства в области информационной безопасности

Как уже отмечалось, самое важное (и, вероятно, самое трудное) на законодательном уровне - создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Пока такого механизма нет и, увы, не предвидится. Сейчас бессмысленно задаваться вопросом, чего не хватает российскому законодательству в области ИБ, это все равно что интересоваться у пунктирного отрезка, чего тому не хватает, чтобы покрыть всю плоскость. Даже чисто количественное сопоставление с законодательством США показывает, что наша законодательная база явно неполна.

Справедливости ради необходимо отметить, что ограничительная составляющая в российском законодательстве представлена существенно лучше, чем координирующая и направляющая. Глава 28 Уголовного кодекса достаточно полно охватывает основные аспекты информационной безопасности, однако обеспечить реализацию соответствующих статей пока еще сложно.

Положения базового Закона "Об информации, информатизации и защите информации" носят весьма общий характер, а основное содержание статей, посвященных информационной безопасности, сводится к необходимости использовать исключительно сертифицированные средства, что, в общем, правильно, но далеко не достаточно. Характерно, что Закон разъясняет вопросы ответственности в случае использования несертифицированных средств, но что делать, если нарушение ИБ произошло в системе, построенной строго по правилам? Кто возместит ущерб субъектам информационных отношений? Поучителен в этом отношении рассмотренный выше закон ФРГ о защите данных.

Законодательством определены органы, ведающие лицензированием и сертификацией. (Отметим в этой связи, что Россия - одна из немногих стран (в список еще входят Вьетнам, Китай, Пакистан), сохранивших жесткий государственный контроль за производством и распространением внутри страны средств обеспечения ИБ, в особенности продуктов криптографических технологий.) Но кто координирует, финансирует и направляет проведение исследований в области ИБ, разработку отечественных средств защиты, адаптацию зарубежных продуктов? Законодательством США определена главная ответственная организация - НИСТ, которая исправно выполняет свою роль. В Великобритании имеются содержательные добровольные стандарты ИБ, помогающие организациям всех размеров и форм собственности. У нас пока ничего такого нет.

В области информационной безопасности законы реально преломляются и работают через нормативные документы, подготовленные соответствующими ведомствами. В этой связи очень важны Руководящие документы Гостехкомиссии России, определяющие требования к классам защищенности средств вычислительной техники и автоматизированных систем. Особенно выделим утвержденный в июле 1997 года Руководящий документ по межсетевым экранам, вводящий в официальную сферу один из самых современных классов защитных средств.

В современном мире глобальных сетей нормативно-правовая база должна быть согласована с международной практикой. Особое внимание следует обратить на то, что желательно привести российские стандарты и сертификационные нормативы в соответствие с международным уровнем информационных технологий вообще и информационной безопасности в частности. Есть целый ряд оснований для того, чтобы это сделать. Одно из них - необходимость защищенного взаимодействия с зарубежными организациями и зарубежными филиалами российских компаний. Второе (более существенное) - доминирование аппаратно-программных продуктов зарубежного производства.

На законодательном уровне должен быть решен вопрос об отношении к таким изделиям. Здесь необходимо выделить два аспекта: независимость в области информационных технологий и информационную безопасность. Использование зарубежных продуктов в некоторых критически важных системах (в первую очередь, военных), в принципе, может представлять угрозу национальной безопасности (в том числе информационной), поскольку нельзя исключить вероятности встраивания закладных элементов. В то же время, в подавляющем большинстве случаев потенциальные угрозы информационной безопасности носят исключительно внутренний характер. В таких условиях незаконность использования зарубежных разработок (ввиду сложностей с их сертификацией) при отсутствии отечественных аналогов затрудняет (или вообще делает невозможной) защиту информации без серьезных на то оснований.

Проблема сертификации аппаратно-программных продуктов зарубежного производства действительно сложна, однако, как показывает опыт европейских стран, решить ее можно. Сложившаяся в Европе система сертификации по требованиям информационной безопасности позволила оценить операционные системы, системы управления базами данных и другие разработки американских компаний. Вхождение России в эту систему и участие российских специалистов в сертификационных испытаниях в состоянии снять имеющееся противоречие между независимостью в области информационных технологий и информационной безопасностью без какого-либо ущерба для национальной безопасности.

Подводя итог, можно наметить следующие основные направления деятельности на законодательном уровне:

- **разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;**
- **обеспечение баланса созидательных и ограничительных (в первую очередь преследующих цель наказать виновных) законов;**
- **интеграция в мировое правовое пространство;**
- **учет современного состояния информационных технологий.**

Лекция 4. Стандарты и спецификации в области информационной безопасности

Основные понятия

Мы приступаем к обзору стандартов и спецификаций двух разных видов:

- оценочных стандартов, направленных на классификацию информационных систем и средств защиты по требованиям безопасности;
- технических спецификаций, регламентирующих различные аспекты реализации средств защиты.

Важно отметить, что между эти видами нормативных документов нет глухой стены. Оценочные стандарты выделяют важнейшие, с точки зрения ИБ, аспекты ИС, играя роль архитектурных спецификаций. Другие технические спецификации определяют, как строить ИС предписанной архитектуры.

Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем".

Данный труд, называемый чаще всего по цвету обложки **"Оранжевой книгой"**, впервые опубликован в августе 1983 года. Уже одно его название требует комментария. Речь идет не о безопасных, а о доверенных системах, то есть системах, которым можно оказать определенную степень доверия.

"Оранжевая книга" поясняет понятие безопасной системы, которая "управляет, с помощью соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию".

Очевидно, однако, что абсолютно безопасных систем не существует, это абстракция. Есть смысл оценивать лишь степень доверия, которое можно оказать той или иной системе.

В "Оранжевой книге" доверенная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

Обратим внимание, что в рассматриваемых Критериях и безопасность, и доверие оцениваются исключительно с точки зрения управления доступом к данным, что является одним из средств обеспечения конфиденциальности и целостности (статической). Вопросы доступности "Оранжевая книга" не затрагивает.

Степень доверия оценивается по двум основным критериям.

1. **Политика безопасности** - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. **Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности.** В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности - это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.
2. **Уровень гарантированности** - мера доверия, которая может быть оказана архитектуре и реализации ИС. Доверие безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. Это пассивный аспект защиты.

Важным средством обеспечения безопасности является механизм подотчетности (протоколирования). Доверенная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть анализом регистрационной информации.

Концепция доверенной вычислительной базы является центральной при оценке степени доверия безопасности. Доверенная вычислительная база - это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности. Качество вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит системный администратор.

Вообще говоря, компоненты вне вычислительной базы могут не быть доверенными, однако это не должно влиять на безопасность системы в целом. В результате, для оценки доверия безопасности ИС достаточно рассмотреть только ее вычислительную базу, которая, как можно надеяться, достаточно компактна.

Основное назначение доверенной вычислительной базы - выполнять функции монитора обращений, то есть контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором действий, допустимых для пользователя.

Монитор обращений должен обладать тремя качествами:

Изолированность. Необходимо предупредить возможность отслеживания работы монитора.

Полнота. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.

Верифицируемость. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

Реализация монитора обращений называется ядром безопасности. Ядро безопасности - это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.

Границу доверенной вычислительной базы называют периметром безопасности. Как уже указывалось, компоненты, лежащие вне периметра безопасности, вообще говоря, могут не быть доверенными. С развитием распределенных систем понятию "периметр безопасности" все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что находится внутри владений, считается доверенным, а то, что вне, - нет.

Механизмы безопасности

Согласно "Оранжевой книге", политика безопасности должна обязательно включать в себя следующие элементы:

1. произвольное управление доступом;
2. безопасность повторного использования объектов;
3. метки безопасности;
4. принудительное управление доступом.

Произвольное управление доступом (называемое иногда дискреционным) - это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту.

Безопасность повторного использования объектов - важное дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной информации из "мусора". Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и магнитных носителей в целом.

Как мы указывали ранее, современный объектно-ориентированный подход резко сужает область действия данного элемента безопасности, затрудняет его реализацию. То же верно и для интеллектуальных устройств, способных буферизовать большие объемы данных.

Для реализации принудительного управления доступом с субъектами и объектами ассоциируются метки безопасности. Метка субъекта описывает его благонадежность, метка объекта - степень конфиденциальности содержащейся в нем информации.

Согласно "Оранжевой книге", метки безопасности состоят из двух частей - уровня секретности и списка категорий. Уровни секретности образуют упорядоченное множество, категории - неупорядоченное. Назначение последних - описать предметную область, к которой относятся данные.

Принудительное (или мандатное) управление доступом основано на сопоставлении меток безопасности субъекта и объекта.

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен - читать можно только то, что положено.

Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, "конфиденциальный" субъект может записывать данные в секретные файлы, но не может - в несекретные (разумеется, должны также выполняться ограничения на набор категорий).

Описанный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов (даже системных администраторов). После того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа.

Если понимать политику безопасности узко, то есть как правила разграничения доступа, то механизм подотчетности является дополнением подобной политики. Цель подотчетности - в каждый момент времени знать, кто работает в системе и что делает. Средства подотчетности делятся на три категории:

- идентификация и аутентификация;
- предоставление доверенного пути;
- анализ регистрационной информации.

Обычный способ идентификации - ввод имени пользователя при входе в систему. Стандартное средство проверки подлинности (аутентификации) пользователя - пароль.

Доверенный путь связывает пользователя непосредственно с доверенной вычислительной базой, минуя другие, потенциально опасные компоненты ИС. Цель предоставления доверенного пути - дать пользователю возможность убедиться в подлинности обслуживающей его системы.

Анализ регистрационной информации (аудит) имеет дело с действиями (событиями), так или иначе затрагивающими безопасность системы.

Если фиксировать все события, объем регистрационной информации, скорее всего, будет расти слишком быстро, а ее эффективный анализ станет невозможным. "Оранжевая книга" предусматривает наличие средств выборочного протоколирования, как в отношении пользователей (внимательно следить только за подозрительными), так и в отношении событий.

Переходя к пассивным аспектам защиты, укажем, что в "Оранжевой книге" рассматривается два вида гарантированности - операционная и технологическая. Операционная гарантированность относится к архитектурным и реализационным аспектам системы, в то время как технологическая - к методам построения и сопровождения.

Операционная гарантированность включает в себя проверку следующих элементов:

- архитектура системы;
- целостность системы;
- проверка тайных каналов передачи информации;
- доверенное администрирование;
- доверенное восстановление после сбоев.

Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее реализация действительно реализуют избранную политику безопасности.

Технологическая гарантированность охватывает весь жизненный цикл системы, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы исключить утечку информации и нелегальные "закладки".

Классы безопасности

"Критерии ..." Министерства обороны США открыли путь к ранжированию информационных систем по степени доверия безопасности.

В "Оранжевой книге" определяется четыре уровня доверия - D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к системам

предъявляются все более жесткие требования. Уровни С и В подразделяются на классы (С1, С2, В1, В2, В3) с постепенным возрастанием степени доверия.

Всего имеется шесть классов безопасности - С1, С2, В1, В2, В3, А1. Чтобы в результате процедуры сертификации систему можно было отнести к некоторому классу, ее политика безопасности и уровень гарантированности должны удовлетворять заданным требованиям, из которых мы упомянем лишь важнейшие.

Класс С1:

- доверенная вычислительная база должна управлять доступом именованных пользователей к именованным объектам;
- пользователи должны идентифицировать себя, прежде чем выполнять какие-либо иные действия, контролируемые доверенной вычислительной базой. Для аутентификации должен использоваться какой-либо защитный механизм, например пароли. Аутентификационная информация должна быть защищена от несанкционированного доступа;
- доверенная вычислительная база должна поддерживать область для собственного выполнения, защищенную от внешних воздействий (в частности, от изменения команд и/или данных) и от попыток слежения за ходом работы;
- должны быть в наличии аппаратные и/или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов доверенной вычислительной базы;
- защитные механизмы должны быть протестированы на предмет соответствия их поведения системной документации. Тестирование должно подтвердить, что у неавторизованного пользователя нет очевидных способов обойти или разрушить средства защиты доверенной вычислительной базы;
- должны быть описаны подход к безопасности, используемый производителем, и применение этого подхода при реализации доверенной вычислительной базы.

Класс С2 (в дополнение к С1):

- права доступа должны гранулироваться с точностью до пользователя. Все объекты должны подвергаться контролю доступа;
- при выделении хранимого объекта из пула ресурсов доверенной вычислительной базы необходимо ликвидировать все следы его использования;
- каждый пользователь системы должен уникальным образом идентифицироваться. Каждое регистрируемое действие должно ассоциироваться с конкретным пользователем;
- доверенная вычислительная база должна создавать, поддерживать и защищать журнал регистрационной информации, относящейся к доступу к объектам, контролируемым базой;
- тестирование должно подтвердить отсутствие очевидных недостатков в механизмах изоляции ресурсов и защиты регистрационной информации.

Класс В1 (в дополнение к С2):

- доверенная вычислительная база должна управлять метками безопасности, ассоциируемыми с каждым субъектом и хранимым объектом;
- доверенная вычислительная база должна обеспечить реализацию принудительного управления доступом всех субъектов ко всем хранимым объектам;
- доверенная вычислительная база должна обеспечивать взаимную изоляцию процессов путем разделения их адресных пространств;
- группа специалистов, полностью понимающих реализацию доверенной вычислительной базы, должна подвергнуть описание архитектуры, исходные и объектные коды тщательному анализу и тестированию;
- должна существовать неформальная или формальная модель политики безопасности, поддерживаемой доверенной вычислительной базой.

Класс В2 (в дополнение к В1):

- снабжаться метками должны все ресурсы системы (например, ПЗУ), прямо или косвенно доступные субъектам;
- к доверенной вычислительной базе должен поддерживаться доверенный коммуникационный путь для пользователя, выполняющего операции начальной идентификации и аутентификации;
- должна быть предусмотрена возможность регистрации событий, связанных с организацией тайных каналов обмена с памятью;
- доверенная вычислительная база должна быть внутренне структурирована на хорошо определенные, относительно независимые модули;
- системный архитектор должен тщательно проанализировать возможности организации тайных каналов обмена с памятью и оценить максимальную пропускную способность каждого выявленного канала;
- должна быть продемонстрирована относительная устойчивость доверенной вычислительной базы к попыткам проникновения;

- модель политики безопасности должна быть формальной. Для доверенной вычислительной базы должны существовать описательные спецификации верхнего уровня, точно и полно определяющие ее интерфейс;
- в процессе разработки и сопровождения доверенной вычислительной базы должна использоваться система конфигурационного управления, обеспечивающая контроль изменений в описательных спецификациях верхнего уровня, иных архитектурных данных, реализационной документации, исходных текстах, работающей версии объектного кода, тестовых данных и документации;
- тесты должны подтверждать действенность мер по уменьшению пропускной способности тайных каналов передачи информации.

Класс В3 (в дополнение к В2):

- для произвольного управления доступом должны обязательно использоваться списки управления доступом с указанием разрешенных режимов;
- должна быть предусмотрена возможность регистрации появления или накопления событий, несущих угрозу политике безопасности системы. Администратор безопасности должен немедленно извещаться о попытках нарушения политики безопасности, а система, в случае продолжения попыток, должна пресекать их наименее болезненным способом;
- доверенная вычислительная база должна быть спроектирована и структурирована таким образом, чтобы использовать полный и концептуально простой защитный механизм с точно определенной семантикой;
- процедура анализа должна быть выполнена для временных тайных каналов;
- должна быть специфицирована роль администратора безопасности. Получить права администратора безопасности можно только после выполнения явных, протоколируемых действий;
- должны существовать процедуры и/или механизмы, позволяющие произвести восстановление после сбоя или иного нарушения работы без ослабления защиты;
- должна быть продемонстрирована устойчивость доверенной вычислительной базы к попыткам проникновения.

Класс А1 (в дополнение к В3):

- тестирование должно продемонстрировать, что реализация доверенной вычислительной базы соответствует формальным спецификациям верхнего уровня;
- помимо описательных, должны быть представлены формальные спецификации верхнего уровня. Необходимо использовать современные методы формальной спецификации и верификации систем;
- механизм конфигурационного управления должен распространяться на весь жизненный цикл и все компоненты системы, имеющие отношение к обеспечению безопасности;
- должно быть описано соответствие между формальными спецификациями верхнего уровня и исходными текстами.

Такова классификация, введенная в "Оранжевой книге". Коротко ее можно сформулировать так:

- уровень С - произвольное управление доступом;
- уровень В - принудительное управление доступом;
- уровень А - верифицируемая безопасность.

Публикация "Оранжевой книги" без всякого преувеличения стала эпохальным событием в области информационной безопасности. **Появился общепризнанный понятийный базис, без которого даже обсуждение проблем ИБ было бы затруднительным.**

Отметим, что огромный идейный потенциал "Оранжевой книги" пока во многом остается невостребованным. Прежде всего это касается концепции технологической гарантированности, охватывающей весь жизненный цикл системы - от выработки спецификаций до фазы эксплуатации.

Информационная безопасность распределенных систем. Рекомендации Х.800

Сетевые сервисы безопасности

Переходим к рассмотрению технической спецификации Х.800, появившейся немногим позднее "Оранжевой книги", но весьма полно и глубоко трактующей вопросы информационной безопасности распределенных систем.

Рекомендации Х.800 - документ довольно обширный. Мы остановимся на специфических сетевых функциях (сервисах) безопасности, а также на необходимых для их реализации защитных механизмах.

Выделяют следующие сервисы безопасности и исполняемые ими роли:

Аутентификация. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и, быть может, периодически во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

Управление доступом. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

Конфиденциальность данных. Обеспечивает защиту от несанкционированного получения информации. Отдельно упомянем конфиденциальность трафика (это защита информации, которую можно получить, анализируя сетевые потоки данных).

Целостность данных подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры - с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

Неотказуемость (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки. Побочным продуктом неотказуемости является аутентификация источника данных.

В следующей таблице указаны уровни эталонной семиуровневой модели OSI, на которых могут быть реализованы функции безопасности. Отметим, что прикладные процессы, в принципе, могут взять на себя поддержку всех защитных сервисов.

Распределение функций безопасности по уровням эталонной семиуровневой модели OSI

Функции безопасности	Уровень 1	Уровень 2	Уровень 3	Уровень 4	Уровень 5	Уровень 6	Уровень 7
Аутентификация	-	-	+	+	-	-	+
Управление доступом	-	-	+	+	-	-	+
Конфиденциальность соединения	+	+	+	+	-	+	+
Конфиденциальность вне соединения	-	+	+	+	-	+	+
Избирательная конфиденциальность	-	-	-	-	-	+	+
Конфиденциальность трафика	+	-	+	-	-	-	+
Целостность с восстановлением	-	-	-	+	-	-	+
Целостность без восстановления	-	-	+	+	-	-	+
Избирательная целостность	-	-	-	-	-	-	+
Целостность вне соединения	-	-	+	+	-	-	+
Неотказуемость	-	-	-	-	-	-	+

"+" данный уровень может предоставить функцию безопасности;

"-" данный уровень не подходит для предоставления функции безопасности.

Сетевые механизмы безопасности

Для реализации сервисов (функций) безопасности могут использоваться следующие механизмы и их комбинации:

- шифрование;
- электронная цифровая подпись;
- механизмы управления доступом. Могут располагаться на любой из участвующих в общении сторон или в промежуточной точке;
- механизмы контроля целостности данных. В рекомендациях X.800 различаются два аспекта целостности: целостность отдельного сообщения или поля информации и целостность потока сообщений или полей информации. Для проверки целостности потока сообщений (то есть для защиты от кражи, переупорядочивания, дублирования и вставки сообщений) используются порядковые номера, временные штампы, криптографическое связывание или иные аналогичные приемы;
- механизмы аутентификации. Согласно рекомендациям X.800, аутентификация может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов, устройств измерения и анализа биометрических характеристик;
- механизмы дополнения трафика;
- механизмы управления маршрутизацией. Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять метка безопасности, ассоциированная с передаваемыми данными;
- механизмы нотаризации. Служат для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, обладающей достаточной информацией. Обычно нотаризация опирается на механизм электронной подписи.

В следующей таблице сведены сервисы (функции) и механизмы безопасности. Таблица показывает, какие механизмы (по отдельности или в комбинации с другими) могут использоваться для реализации той или иной функции.

Взаимосвязь функций и механизмов безопасности Функции Механизмы

Функции	Механизмы							
	Шифрование	Электронная подпись	Управление доступом	Целостность	Аутентификация	Дополнение трафика	Управление маршрутизацией	Нотаризация
Аутентификация партнеров	+	+	-	-	+	-	-	-
Аутентификация источника	+	+	-	-	-	-	-	-
Управление доступом	-	-	+	-	-	-	-	-
Конфиденциальность	+	-	+	-	-	-	+	-
Избирательная конфиденциальность	+	-	-	-	-	-	-	-
Конфиденциальность трафика	+	-	-	-	-	+	+	-
Целостность соединения	+	-	-	+	-	-	-	-
Целостность вне соединения	+	+	-	+	-	-	-	-
Неотказуемость	-	+	-	+	-	-	-	+

"+" механизм пригоден для реализации данной функцию безопасности;

"-" механизм не предназначен для реализации данной функции безопасности.

Администрирование средств безопасности

Администрирование средств безопасности включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Примерами могут служить распространение криптографических ключей, установка значений параметров защиты, ведение регистрационного журнала и т.п.

Концептуальной основой администрирования является информационная база управления безопасностью. Эта база может не существовать как единое (распределенное) хранилище, но каждая из оконечных систем должна располагать информацией, необходимой для реализации избранной политики безопасности.

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям:

- администрирование информационной системы в целом;
- администрирование сервисов безопасности;
- администрирование механизмов безопасности.

Среди действий, относящихся к ИС в целом, отметим обеспечение актуальности политики безопасности, взаимодействие с другими административными службами, реагирование на происходящие события, аудит и безопасное восстановление.

Администрирование сервисов безопасности включает в себя определение защищаемых объектов, выработку правил подбора механизмов безопасности (при наличии альтернатив), комбинирование механизмов для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Обязанности администратора механизмов безопасности определяются перечнем задействованных механизмов. Типичный список таков:

- управление ключами (генерация и распределение);
- управление шифрованием (установка и синхронизация криптографических параметров).

К управлению шифрованием можно отнести и администрирование механизмов электронной подписи. Управление целостностью, если оно обеспечивается криптографическими средствами, также тяготеет к данному направлению;

- администрирование управления доступом (распределение информации, необходимой для управления - паролей, списков доступа и т.п.);
- управление аутентификацией (распределение информации, необходимой для аутентификации - паролей, ключей и т.п.);
- управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений - частоту отправки, размер и т.п.);
- управление маршрутизацией (выделение доверенных путей);
- управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

Мы видим, что администрирование средств безопасности в распределенной ИС имеет много особенностей по сравнению с централизованными системами.

Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий". Основные понятия.

Мы возвращаемся к теме оценочных стандартов, приступая к рассмотрению самого полного и современного среди них - "Критериев оценки безопасности информационных технологий" (издан 1

декабря 1999 года). Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба.

По историческим причинам данный стандарт часто называют "Общими критериями" (или даже ОК). Мы также будем использовать это сокращение.

"Общие критерии" на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. В отличие от "Оранжевой книги", ОК не содержат предопределенных "классов безопасности". Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.

С программистской точки зрения ОК можно считать набором библиотек, помогающих писать содержательные "программы" - задания по безопасности, типовые профили защиты и т.п. Программисты знают, насколько хорошая библиотека упрощает разработку программ, повышает их качество. Без библиотек, "с нуля", программы не пишут уже очень давно; оценка безопасности тоже вышла на сопоставимый уровень сложности, и "Общие критерии" предоставили соответствующий инструментарий.

Важно отметить, что требования могут быть параметризованы, как и полагается библиотечным функциям.

Как и "Оранжевая книга", ОК содержат два основных вида требований безопасности:

- функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;
- требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Требования безопасности предъявляются, а их выполнение проверяется для определенного **объекта оценки** - аппаратно-программного продукта или информационной системы.

Очень важно, что безопасность в ОК рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

- определение назначения, условий применения, целей и требований безопасности;
- проектирование и разработка;
- испытания, оценка и сертификация;
- внедрение и эксплуатация.

В ОК объект оценки рассматривается в контексте среды безопасности, которая характеризуется определенными условиями и угрозами.

В свою очередь, угрозы характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

Уязвимые места могут возникать из-за недостатка в:

- требованиях безопасности;
- проектировании;
- эксплуатации.

Слабые места по возможности следует устранить, минимизировать или хотя бы постараться ограничить возможный ущерб от их преднамеренного использования или случайной активизации.

С точки зрения технологии программирования в ОК использован устаревший библиотечный (не объектный) подход. Чтобы, тем не менее, структурировать пространство требований, в "Общих критериях" введена иерархия класс-семейство-компонент-элемент.

Классы определяют наиболее общую, "предметную" группировку требований (например, функциональные требования подотчетности).

Семейства в пределах класса различаются по строгости и другим нюансам требований.

Компонент - минимальный набор требований, фигурирующий как целое.

Элемент - неделимое требование.

Как и между библиотечными функциями, между компонентами ОК могут существовать зависимости. Они возникают, когда компонент сам по себе недостаточен для достижения цели безопасности. Вообще говоря, не все комбинации компонентов имеют смысл, и понятие зависимости в какой-то степени компенсирует недостаточную выразительность библиотечной организации, хотя и не заменяет объединение функций в содержательные объектные интерфейсы.

Как указывалось выше, с помощью библиотек могут формироваться два вида нормативных документов: профиль защиты и задание по безопасности.

Профиль защиты (ПЗ) представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

Задание по безопасности содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

Выше мы отмечали, что в ОК нет готовых классов защиты. Сформировать классификацию в терминах "Общих критериев" - значит определить несколько иерархически упорядоченных (содержащих усиливающиеся требования) профилей защиты, в максимально возможной степени использующих стандартные функциональные требования и требования доверия безопасности.

Выделение некоторого подмножества из всего множества профилей защиты во многом носит субъективный характер. По целому ряду соображений (одним из которых является желание придерживаться объектно-ориентированного подхода) целесообразно, на наш взгляд, сформировать сначала отправную точку классификации, выделив базовый (минимальный) ПЗ, а дополнительные требования компоновать в функциональные пакеты.

Функциональный пакет - это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности. "Общие критерии" не регламентируют структуру пакетов, процедуры верификации, регистрации и т.п., отводя им роль технологического средства формирования ПЗ.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

Функциональные требования

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в "Общих критериях" представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это, конечно, значительно больше, чем число аналогичных сущностей в "Оранжевой книге".

Перечислим классы функциональных требований ОК:

- идентификация и аутентификация;
- защита данных пользователя;
- защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
- управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
- аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
- доступ к объекту оценки;
- приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
- использование ресурсов (требования к доступности информации);
- криптографическая поддержка (управление ключами);
- связь (аутентификация сторон, участвующих в обмене данными);
- доверенный маршрут/канал (для связи с сервисами безопасности).

Опишем подробнее два класса, демонстрирующие особенности современного подхода к ИБ.

Класс "Приватность" содержит 4 семейства функциональных требований.

Анонимность. Позволяет выполнять действия без раскрытия идентификатора пользователя другим пользователям, субъектам и/или объектам. Анонимность может быть полной или выборочной. В последнем случае она может относиться не ко всем операциям и/или не ко всем пользователям (например, у уполномоченного пользователя может оставаться возможность выяснения идентификаторов пользователей).

Псевдонимность. Напоминает анонимность, но при применении псевдонима поддерживается ссылка на идентификатор пользователя для обеспечения подотчетности или для других целей.

Невозможность ассоциации. Семейство обеспечивает возможность неоднократного использования информационных сервисов, но не позволяет ассоциировать случаи использования между собой и приписать их одному лицу. Невозможность ассоциации защищает от построения профилей поведения пользователей (и, следовательно, от получения информации на основе подобных профилей).

Скрытность. Требования данного семейства направлены на то, чтобы можно было использовать информационный сервис с сокрытием факта использования. Для реализации скрытности может применяться, например, широковещательное распространение информации, без указания конкретного адресата. Годятся для реализации скрытности и методы стеганографии, когда скрывается не только содержание сообщения (как в криптографии), но и сам факт его отправки.

Еще один показательный (с нашей точки зрения) класс функциональных требований - "Использование ресурсов", содержащий требования доступности. Он включает три семейства.

Отказоустойчивость. Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В ОК различаются активная и пассивная отказоустойчивость. Активный механизм содержит специальные функции, которые активизируются в случае сбоя. Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.

Обслуживание по приоритетам. Выполнение этих требований позволяет управлять использованием ресурсов так, что низкоприоритетные операции не могут помешать высокоприоритетным.

Распределение ресурсов. Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.

Мы видим, что "Общие критерии" - очень продуманный и полный документ с точки зрения функциональных требований. В то же время, хотелось бы обратить внимание и на некоторые недостатки.

Первый мы уже отмечали - это отсутствие объектного подхода. Функциональные требования не сгруппированы в осмысленные наборы (объектные интерфейсы), к которым могло бы применяться наследование. Подобное положение, как известно из технологии программирования, чревато появлением слишком большого числа комбинаций функциональных компонентов, несопоставимых между собой.

В современном программировании ключевым является вопрос накопления и многократного использования знаний. Стандарты - одна из форм накопления знаний. Следование в ОК "библиотечному", а не объектному подходу сужает круг фиксируемых знаний, усложняет их корректное использование.

К сожалению, в "Общих критериях" отсутствуют архитектурные требования, что является естественным следствием избранного старомодного программистского подхода "снизу вверх". На наш взгляд, это серьезное упущение. Технологичность средств безопасности, следование общепризнанным рекомендациям по протоколам и программным интерфейсам, а также апробированным архитектурным решениям, таким как менеджер/агент, - необходимые качества изделий информационных технологий, предназначенных для поддержки критически важных функций, к числу которых, безусловно, относятся функции безопасности. Без рассмотрения интерфейсных аспектов системы оказываются нерасширяемыми и изолированными. Очевидно, с практической точки зрения это недопустимо. В то же время, обеспечение безопасности интерфейсов - важная задача, которую желательно решать единообразно.

Требования доверия безопасности

Установление доверия безопасности, согласно "Общим критериям", основывается на активном исследовании объекта оценки.

Форма представления требований доверия, в принципе, та же, что и для функциональных требований. Специфика состоит в том, что каждый элемент требований доверия принадлежит одному из трех типов:

- действия разработчиков;
- представление и содержание свидетельств;
- действия оценщиков.

Всего в ОК 10 классов, 44 семейства, 93 компонента требований доверия безопасности. Перечислим классы:

- разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);
- поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);
- тестирование;
- оценка уязвимостей (включая оценку стойкости функций безопасности);
- поставка и эксплуатация;
- управление конфигурацией;
- руководства (требования к эксплуатационной документации);
- поддержка доверия (для поддержки этапов жизненного цикла после сертификации);
- оценка профиля защиты;
- оценка задания по безопасности.

Применительно к требованиям доверия в "Общих критериях" сделана весьма полезная вещь, не реализованная, к сожалению, для функциональных требований. А именно, введены так называемые оценочные уровни доверия (их семь), содержащие осмысленные комбинации компонентов.

Оценочный уровень доверия 1 (начальный) предусматривает анализ функциональной спецификации, спецификации интерфейсов, эксплуатационной документации, а также независимое тестирование. Уровень применим, когда угрозы не рассматриваются как серьезные.

Оценочный уровень доверия 2, в дополнение к первому уровню, предусматривает наличие проекта верхнего уровня объекта оценки, выборочное независимое тестирование, анализ стойкости функций безопасности, поиск разработчиком явных уязвимых мест.

На третьем уровне ведется контроль среды разработки и управление конфигурацией объекта оценки.

На уровне 4 добавляются полная спецификация интерфейсов, проекты нижнего уровня, анализ подмножества реализации, применение неформальной модели политики безопасности, независимый анализ уязвимых мест, автоматизация управления конфигурацией. Вероятно, это самый высокий уровень, которого можно достичь при существующей технологии программирования и приемлемых затратах.

Уровень 5, в дополнение к предыдущим, предусматривает применение формальной модели политики безопасности, полуформальных функциональной спецификации и проекта верхнего уровня с демонстрацией соответствия между ними. Необходимо проведение анализа скрытых каналов разработчиками и оценщиками.

На уровне 6 реализация должна быть представлена в структурированном виде. Анализ соответствия распространяется на проект нижнего уровня.

Оценочный уровень 7 (самый высокий) предусматривает формальную верификацию проекта объекта оценки. Он применим к ситуациям чрезвычайно высокого риска.

На этом мы заканчиваем краткий обзор "Общих критериев".

Гармонизированные критерии Европейских стран

Наше изложение "Гармонизированных критериев" основывается на версии 1.2, опубликованной в июне 1991 года от имени соответствующих органов четырех стран - Франции, Германии, Нидерландов и Великобритании.

Принципиально важной чертой Европейских Критериев является отсутствие требований к условиям, в которых должна работать информационная система. Так называемый спонсор, то есть организация, запрашивающая сертификационные услуги, формулирует цель оценки, то есть описывает условия, в которых должна работать система, возможные угрозы ее безопасности и предоставляемые ею защитные функции. Задача органа сертификации - оценить, насколько полно достигаются поставленные цели, то есть насколько корректны и эффективны архитектура и реализация механизмов безопасности в описанных спонсором условиях. Таким образом, в терминологии "Оранжевой книги", Европейские Критерии относятся к гарантированности безопасной работы системы. Требования к политике безопасности и наличию защитных механизмов не являются составной частью Критериев. Впрочем, чтобы облегчить формулировку цели оценки, Критерии содержат в качестве приложения описание десяти классов функциональности, типичных для правительственных и коммерческих систем.

Европейские Критерии рассматривают все основные составляющие информационной безопасности - конфиденциальность, целостность, доступность.

В Критериях проводится различие между системами и продуктами. Система - это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении. Продукт - это аппаратно-программный "пакет", который можно купить и по своему усмотрению встроить в ту или иную систему. Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях.

Из практических соображений важно обеспечить единство критериев оценки продуктов и систем - например, чтобы облегчить оценку системы, составленной из ранее сертифицированных продуктов. По этой причине для систем и продуктов вводится единый термин - объект оценки.

Каждая система и/или продукт предъявляет свои требования к обеспечению конфиденциальности, целостности и доступности. Чтобы удовлетворить эти требования, необходимо предоставить соответствующий набор функций (сервисов) безопасности, таких как идентификация и аутентификация, управление доступом или восстановление после сбоев.

Сервисы безопасности реализуются посредством конкретных механизмов. Чтобы объекту оценки можно было доверять, необходима определенная степень уверенности в наборе функций и механизмов безопасности. Степень уверенности мы будем называть гарантированностью. Гарантированность может быть большей или меньшей в зависимости от тщательности проведения оценки.

Гарантированность затрагивает два аспекта - эффективность и корректность средств безопасности. При проверке эффективности анализируется соответствие между целями, сформулированными для объекта оценки, и имеющимся набором функций безопасности. Точнее говоря, рассматриваются вопросы адекватности функциональности, взаимной согласованности функций, простоты их использования, а также возможные последствия эксплуатации известных слабых мест защиты. Кроме того, в понятие эффективности входит способность механизмов защиты противостоять прямым атакам (мощность механизма). Определяются три градации мощности - базовая, средняя и высокая.

Под корректностью понимается правильность реализации функций и механизмов безопасности. В Критериях определяется семь возможных уровней гарантированности корректности - от E0 до E6 (в порядке возрастания). Уровень E0 означает отсутствие гарантированности. При проверке корректности анализируется весь жизненный цикл объекта оценки - от проектирования до эксплуатации и сопровождения.

Общая оценка системы складывается из минимальной мощности механизмов безопасности и уровня гарантированности корректности.

Гармонизированные критерии Европейских стран явились для своего времени весьма передовым стандартом, они создали предпосылки для появления "Общих критериев".

Интерпретация "Оранжевой книги" для сетевых конфигураций

В 1987 году Национальным центром компьютерной безопасности США была опубликована интерпретация "Оранжевой книги" для сетевых конфигураций. Данный документ состоит из двух частей. Первая содержит собственно интерпретацию, во второй рассматриваются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

В первой части вводится минимум новых понятий. Важнейшее из них - сетевая доверенная вычислительная база, распределенный аналог доверенной вычислительной базы изолированных систем. Сетевая доверенная вычислительная база формируется из всех частей всех компонентов сети, обеспечивающих информационную безопасность. Доверенная сетевая система должна обеспечивать такое распределение защитных механизмов, чтобы общая политика безопасности реализовывалась, несмотря на уязвимость коммуникационных путей и на параллельную, асинхронную работу компонентов.

Прямой зависимости между вычислительными базами компонентов, рассматриваемых как изолированные системы, и фрагментами сетевой вычислительной базы не существует. Более того, нет прямой зависимости и между уровнями безопасности отдельных компонентов и уровнем безопасности всей сетевой конфигурации. Например, в результате объединения двух систем класса B1, обладающих несовместимыми правилами кодирования меток безопасности, получается сеть, не удовлетворяющая требованию целостности меток. В качестве противоположного примера рассмотрим объединение двух компонентов, один из которых сам не обеспечивает протоколирование действий пользователя, но передает необходимую информацию другому компоненту, который и ведет протокол. В таком случае распределенная система в целом, несмотря на слабость компонента, удовлетворяет требованию подотчетности.

Чтобы понять суть положений, вошедших в первую часть, рассмотрим интерпретацию требований к классу безопасности C2. Первое требование к этому классу - поддержка произвольного управления доступом. Интерпретация предусматривает различные варианты распределения сетевой доверенной вычислительной базы по компонентам и, соответственно, различные варианты распределения механизмов управления доступом. В частности, некоторые компоненты, закрытые для прямого доступа пользователей, могут вообще не содержать подобных механизмов.

Интерпретация отличается от самих "Критериев" учетом динамичности сетевых конфигураций. Предусматривается наличие средств проверки подлинности и корректности функционирования компонентов перед их включением в сеть, наличие протокола взаимной проверки компонентами корректности функционирования друг друга, а также присутствие средств оповещения администратора о неполадках в сети. Сетевая конфигурация должна быть устойчива к отказам отдельных компонентов или коммуникационных путей.

Среди защитных механизмов в сетевых конфигурациях на первом месте стоит криптография, помогающая поддерживать как конфиденциальность, так и целостность. Следствием использования криптографических методов является необходимость реализации механизмов управления ключами.

Систематическое рассмотрение вопросов доступности является новшеством по сравнению не только с "Оранжевой книгой", но и с рекомендациями X.800. Сетевой сервис перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии обслуживать запросы. Удаленный ресурс может стать недоступным и вследствие нарушения равноправия в обслуживании пользователей. Доверенная система должна иметь возможность обнаруживать ситуации недоступности, уметь возвращаться к нормальной работе и противостоять атакам на доступность.

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

- внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т.п.);
- наличие средств реконфигурирования для изоляции и/или замены узлов или коммуникационных каналов, отказавших или подвергшихся атаке на доступность;
- рассредоточенность сетевого управления, отсутствие единой точки отказа;
- наличие средств нейтрализации отказов (обнаружение отказавших компонентов, оценка последствий, восстановление после отказов);
- выделение подсетей и изоляция групп пользователей друг от друга.

Одним из важнейших в "Оранжевой книге" является понятие монитора обращений. Применительно к структурированию сетевой конфигурации можно сформулировать следующее утверждение, обеспечивающее достаточное условие корректности фрагментирования монитора обращений.

Пусть каждый субъект (то есть процесс, действующий от имени какого-либо пользователя) заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента. Далее, пусть каждый компонент содержит свой монитор обращений, отслеживающий все локальные попытки доступа, и все мониторы реализуют согласованную политику безопасности. Пусть, наконец, коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации. Тогда совокупность всех мониторов образует единый монитор обращений для всей сетевой конфигурации.

Данное утверждение является теоретической основой декомпозиции распределенной ИС в объектно-ориентированном стиле в сочетании с криптографической защитой коммуникаций.

Руководящие документы Гостехкомиссии России

Гостехкомиссия России ведет весьма активную нормотворческую деятельность, выпуская Руководящие документы (РД), играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления Гостехкомиссия России выбрала ориентацию на "Общие критерии", что можно только приветствовать.

В своем обзоре мы рассмотрим два важных, хотя и не новых, Руководящих документа - Классификацию автоматизированных систем (АС) по уровню защищенности от несанкционированного доступа (НСД) и аналогичную Классификацию межсетевых экранов (МЭ).

Согласно первому из них, устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа классифицирует АС, в которых работает один пользователь, имеющий доступ ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранящейся на носителях различного уровня конфиденциальности.

Группа содержит два класса - 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

Сведем в таблицу требования ко всем девяти классам защищенности АС.

Требования к защищенности автоматизированных систем.

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом 1.1. Идентификация, проверка подлинности и контроль доступа субъектов: в систему;	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	-	-	-	+	-	+	+	+	+
к программам;	-	-	-	+	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей.	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации	-	-	-	+	-	-	+	+	+
2. Подсистема регистрации и учета 2.1. Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети);	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов;	-	+	-	+	-	+	+	+	+
запуска/завершения программ и процессов (заданий, задач);	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	-	-	-	+	-	+	+	+	+
изменения полномочий субъектов доступа;	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа.	-	-	-	+	-	+	+	+	+
2.2. Учет носителей информации.	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.	-	+	-	+	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты.	-	-	-	-	-	-	+	+	+
3. Криптографическая подсистема 3.1. Шифрование конфиденциальной информации.	-	-	-	+	-	-	-	+	+
3.2. Шифрование информации, принадлежащей	-	-	-	-	-	-	-	-	+

различным субъектам доступа (группам субъектов) на разных ключах.									
3.3. Использование аттестованных (сертифицированных) криптографических средств.	-	-	-	+	-	-	-	+	+
4. Подсистема обеспечения целостности 4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации.	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы защиты) информации в АС.	-	-	-	+	-	-	+	+	+
4.4. Периодическое тестирование СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты.	-	+	-	+	-	-	+	+	+

"-" нет требований к данному классу;

"+" есть требования к данному классу;

"СЗИ НСД" система защиты информации от несанкционированного доступа

По существу перед нами - минимум требований, которым необходимо следовать, чтобы обеспечить конфиденциальность информации. Целостность представлена отдельной подсистемой (номер 4), но непосредственно к интересующему нас предмету имеет отношение только пункт 4.1. Доступность (точнее, восстановление) предусмотрено только для самих средств защиты.

Переходя к рассмотрению второго РД Гостехкомиссии России - Классификации межсетевых экранов - укажем, что данный РД представляется нам принципиально важным, поскольку в нем идет речь не о целостном продукте или системе, а об отдельном сервисе безопасности, обеспечивающем межсетевое разграничение доступа.

Данный РД важен не столько содержанием, сколько самим фактом своего существования.

Основным критерием классификации МЭ служит протокольный уровень (в соответствии с эталонной семиуровневой моделью), на котором осуществляется фильтрация информации. Это понятно: чем выше уровень, тем больше информации на нем доступно и, следовательно, тем более тонкую и надежную фильтрацию можно реализовать.

Значительное внимание в РД уделено собственной безопасности служб обеспечения защиты и вопросам согласованного администрирования распределенных конфигураций.

Расследование компьютерных преступлений

Расследование компьютерных преступлений существенно отличаются от расследований других "традиционных" преступлений. По данным уголовным делам чаще всего допускаются ошибки, что зачастую объясняется отсутствием надлежащего уровня теоретической и практической подготовки оперативных работников и следователей. Изучение уголовных дел этой категории дает основание полагать, что одной из существенных причин низкого качества следствия является отсутствие систематизированных и отработанных методик расследования компьютерных преступлений, а также ошибки, которые совершаются при проведении следственных действий в отношении компьютерной информации либо самих компьютеров.

Результаты анализа практической деятельности правоохранительных органов по расследованию компьютерных преступлений свидетельствуют о том, что исследование компьютерной техники целесообразно проводить в условиях криминалистической лаборатории, где эту работу выполняют специалисты с необходимой профессиональной подготовкой.

Доказательства, связанные с компьютерными преступлениями и изъятые с места происшествия, могут быть легко изменены, как в результате ошибок при их изъятии, так и в процессе самого исследования. Представление подобных доказательств в судебном процессе требует специальных знаний и соответствующей подготовки. Здесь нельзя недооценивать роль экспертизы, которая может дать квалифицированный ответ на поставленные вопросы.

Однако экспертиза требует какого-то времени не только на ее проведение, но и на поиск соответствующих специалистов, а при изъятии компьютерной техники существенным фактором, позволяющим сохранить необходимую доказательную информацию, является неожиданность и оперативность. Именно поэтому изъятие компьютеров и информации приходится проводить теми силами, которые в настоящее время проводят следственные действия. В данном случае именно следователь не застрахован от ошибок, обусловленных недостаточностью знаний, что потом достаточно умело, используется защитой в суде.

Поставленная проблема имеет два аспекта: общие ошибки, которые допускаются работниками правоохранительных органов при расследовании компьютерных преступлений, и технические аспекты, связанные с защитой информации, которая устанавливается на компьютерах их непосредственными пользователями.

Как известно, обнаружение, осмотр и изъятие компьютеров и компьютерной информации в процессе следственных действий могут совершаться не только при следственном осмотре (ст. 190 КПК), но и при проведении других следственных действий: обыски (ст. 178 КПК); выемки (ст. 179 КПК); воспроизведения обстоятельств и обстановки происшествия (ст.194 КПК).

Следует выделить некоторые правила работы с компьютерами, изъятыми при расследовании преступлений в сфере компьютерной информации, а также предложить общие рекомендации, которые могут быть полезными при обработке компьютерных доказательств.

Рассмотрим некоторые типичные ошибки, наиболее часто совершаемые при проведении следственных действий в отношении компьютерной информации либо самих компьютеров.

Ошибка 1. Ошибочная работа с компьютером.

Первое и основное правило, которое должно неуклонно выполняться, состоит в следующем: никогда и ни при каких условиях не работать на изъятом компьютере. Это правило допускает, что изъятый компьютер - прежде всего объект исследования специалиста. Поэтому до передачи экспертам его желательно даже не включать, поскольку категорически запрещено исполнять любые операции на изъятом компьютере, не обеспечив необходимых мер защиты (например, защиты от модификации или создания резервной копии). Если на компьютере установлена система защиты (например - пароль), то его включение может вызвать уничтожение информации, которая находится на жестком диске. Не допускается загрузка такого компьютера с использованием его собственной операционной системы.

Подобная мера объясняется достаточно просто: преступнику не составляет особого труда установить на своем компьютере программу для уничтожения информации на жестком или гибком магнитном дисках, записав такие "ловушки" через модификацию операционной системы. Например, простая команда DIR, которая используется для отображения каталога диска, может быть легко изменена, чтобы отформатировать жесткий диск.

После того, как данные и сама разрушительная программа уничтожены, никто не сможет сказать наверняка, был ли "подозреваемый" компьютер оборудован такими программами специально, или это результат небрежности при исследовании компьютерных доказательств?

Ошибка 2. Допуск к компьютеру владельца (пользователя) компьютера.

Серьезной ошибкой является допуск к исследуемому компьютеру владельца для оказания помощи в его эксплуатации. Известны многие случаи из практики, когда подозреваемые на допросах, связанных с компьютерными доказательствами, допускались к работе на изъятом компьютере. Позже они рассказывали своим знакомым, как шифровали файлы "прямо под носом у полицейских", а те об этом даже не догадывались. Учитывая такие последствия, компьютерные специалисты стали делать резервные копии компьютерной информации прежде, чем допускать к работе над ней.

Еще одна проблема связанна с возможностью опровержения в суде идентичности предъявленного на процессе программного обеспечения тому, которое находилось на данном компьютере на момент изъятия. Чтобы избежать подобных ситуаций, компьютер, следует опечатать в присутствии понятых, не включая. Если работник правоохранительных органов принимает решение об осмотре компьютера на месте, первое, что необходимо сделать, это снять копию с жесткого магнитного диска и любой дискеты, которая будет изыматься как вещественное доказательство. Это означает, что до проведения каких-либо операций с компьютером, необходимо зафиксировать его состояние на момент проведения следственных действий.

Ошибка 3. Отсутствие проверки компьютера на наличие вирусов и программных закладок.

С целью проверки компьютера на наличие вирусов и программных закладок, необходимо загрузить компьютер не с его операционной системы, а со своей загодя подготовленной дискеты, либо со стендового жесткого диска. Проверке подвергаются все носители информации - дискеты, жесткий диск и другие носители. Эту работу следует проделать привлеченному к участию в следственных действиях специалисту с помощью специального программного обеспечения.

Нельзя допустить, чтобы у суда появилась возможность обвинения следствия в умышленном заражении компьютера вирусами, в некомпетентности при проведении следственных действий, либо просто в небрежности, поскольку доказать, что вирус находился в компьютере до момента исследования, вряд ли возможно, а подобное обвинение поставит под сомнение всю работу эксперта и достоверность его выводов.

Такие наиболее типичные ошибки, которые часто встречаются при исследовании компьютера в делах, связанных с расследованием компьютерных преступлений. Однако рассмотренный перечень не охватывает всех ошибок, возникающих в процессе изъятия и исследования компьютерной информации. Этому можно легко дать объяснение: отсутствие достаточного опыта в подобных делах в нашей стране. В то же время в странах Западной Европы и США уже накоплен богатый опыт расследования сложных компьютерных преступлений. Необходимо более тщательно его изучить, что позволит избежать многих из них.

Во избежание ошибок при проведении следственных действий на начальном этапе расследования, которые могут привести к потере или искажению компьютерной информации, следует придерживаться некоторых предохранительных мер.

Рекомендация 1. В первую очередь следует сделать резервную копию информации.

В процессе обыска и выемки, связанных с изъятием компьютера, магнитных носителей и информации, возникает ряд общих проблем, связанных со спецификой изымаемых технических средств. В первую очередь необходимо предусмотреть меры безопасности, которые совершаются преступниками с целью уничтожения компьютерной информации. Они, например, могут использовать специальное оборудование, в критических случаях образующее сильное магнитное поле, которое стирает магнитные записи.

На протяжении обыска все электронные доказательства, находящиеся в компьютере либо в компьютерной системе должны быть собраны таким образом, дабы они потом могли быть признанными судом. Мировая практика показывает, что в большинстве случае под давлением представителей защиты в суде электронные доказательства не принимаются во внимание. Чтобы гарантировать их признание в качестве доказательств, необходимо строго придерживаться уголовно-процессуального законодательства, а также стандартизированных приемов и методик их изъятия.

Обычно компьютерные доказательства сохраняются путем создания точной копии с оригинала (первичного доказательства), прежде чем делается какой-либо их анализ. Но делать копии компьютерных файлов, используя только стандартные программы резервного копирования, недостаточно. Вещественные доказательства могут существовать в виде уничтоженных либо спрятанных файлов, а данные, связанные с этими файлами, можно сохранить только с помощью специального программного обеспечения. В самом простом виде это могут быть программы типа - SafeBack, а для гибких дискет бывает достаточно программы DOS Discopy.

Магнитные носители, на которые предусматривается копировать информацию, должны быть заранее подготовленные (необходимо убедиться, что на них отсутствует какая-нибудь информация). Носители следует сохранять в специальных упаковках либо заворачивать в чистую бумагу. Необходимо помнить, что информация может быть повреждена влажностью, температурным влиянием или электростатическими (магнитными) полями.

Рекомендация 2. Найти и сделать копии временных файлов.

Многие текстовые редакторы и программы управления базами данных создают временные файлы как побочный продукт нормальной работы программного обеспечения. Большинство пользователей компьютера не осознают важности создания этих файлов, потому что обычно они уничтожаются программой в конце сеанса работы. Однако данные, находящиеся внутри этих уничтоженных файлов, могут оказаться наиболее полезными. Особенно, если исходный файл был кодированный или документ подготовки текстов был напечатан, но никогда не сохранялся на диске, такие файлы могут быть восстановлены.

Рекомендация 3. Необходимо обязательно проверить Swap File.

Популярность Microsoft Windows принесла некоторые дополнительные средства, касающиеся исследования компьютерной информации. Swap File функционируют как дисковая память, огромная база данных и множество разных временных фрагментов информации. В этом Swap File может быть обнаружен даже весь текст документа.

Рекомендация 4. Необходимо сравнивать дубли текстовых документов.

Часто дубли текстовых файлов можно обнаружить на жестком либо гибком магнитных дисках. Это могут быть незначительные изменения между версиями одного документа, которые могут иметь доказательную ценность. Расхождения можно легко идентифицировать с помощью наиболее современных текстовых редакторов.

Хотелось бы выделить также общие рекомендации, которые необходимо учитывать при исследовании компьютера на месте происшествия.

Приступая к осмотру компьютера, следователь и специалист, непосредственно производящий все действия на ЭВМ, должны придерживаться следующего:

- перед выключением компьютера необходимо по возможности закрыть все используемые на компьютере программы. Следует помнить о том, что некорректный выход с некоторых программ может вызвать уничтожение информации или испортить саму программу;
- принять меры по установлению пароля доступа к защищенным программам;
- при активном вмешательстве сотрудников предприятия, стремящихся противодействовать следственной группе, необходимо отключить электропитание всех компьютеров на объекте, опечатать их и изъять вместе с магнитными носителями для исследования информации в лабораторных условиях;
- в случае необходимости консультаций персонала предприятия, получать их следует у разных лиц путем опрашивания или допроса. Подобный метод позволит получить максимально правдивую информацию и избежать умышленного вреда;
- при изъятии технических средств, целесообразно изымать не только системные блоки, но и дополнительные периферийные устройства (принтеры, стримеры, модемы, сканеры и т.п.);
- при наличии локальной вычислительной сети необходимо иметь нужное количество специалистов для дополнительного исследования информационной сети;
- изымать все компьютеры (системные блоки) и магнитные носители;

- тщательно осмотреть документацию, обращая внимание на рабочие записи операторов ЭВМ, ибо часто именно в этих записях неопытных пользователей можно обнаружить коды, пароли и другую полезную информацию;
- составить список всех внештатных и временных работников организации (предприятия) с целью выявления программистов и других специалистов в области информационных технологий, работающих в данном учреждении. Желательно установить их паспортные данные, адреса и места постоянной работы;
- записать данные всех лиц, находящихся в помещении на момент появления следственной группы, независимо от объяснения причин их пребывания в данном помещении;
- составить список всех сотрудников предприятия, имеющих доступ к компьютерной технике либо часто пребывающих в помещении, где находятся ЭВМ.

Если возможен непосредственный доступ к компьютеру и исключены все нежелательные ситуации, приступают к осмотру. Причем следователь и специалист должны четко объяснять все свои действия понятым.

При осмотре должны быть установлены:

- конфигурация компьютера с четким и подробным описанием всех устройств;
- номера моделей и серийные номера каждого из устройств;
- инвентарные номера, присваиваемые бухгалтерией при постановке оборудования на баланс предприятия;
- другая информация с фабричных ярлыков (на клавиатуре ярлык обычно находится на обратной стороне, а на мониторе и процессоре - сзади). Такая информация вносится в протокол осмотра вычислительной техники и может быть важной для следствия.

Рекомендация 5. Фотографирование и маркирование элементов компьютерной системы.

Фотографирование и маркирование элементов компьютерной системы - важный первый шаг при подготовке системы к транспортировке. Документирование состояния системы на данном этапе необходимо для правильной сборки и подключения всех элементов системы в условиях лаборатории. При фотографировании следует исполнить снимки системы крупным планом ее передней и задней частей. Фотографирование и маркирование элементов изымаемой компьютерной системы дает возможность в точности воссоздать состояние компьютерной техники в лабораторных условиях исследования. Некоторое оборудование типа внешних модемов может иметь множество мелких переключателей, фиксирующих его состояние, которые при транспортировке могут быть изменены, что создаст дополнительные проблемы для эксперта.

В заключение необходимо подчеркнуть, что при проведении любых следственных действий, связанных с расследованием преступлений в сфере использования компьютерных технологий (особенно выемка информации и компьютерного оборудования) целесообразно с самого начала привлечение специалиста в области информационных технологий. До начала следственных действий следует также иметь определенную информацию, касающуюся: марки, модели, компьютера, операционной системы, периферийных устройств, средств связи и любые другие ведомости о системе, которая является объектом расследования. Целенаправленная деятельность следователя, оперативных работников, особенно на первичном этапе расследования, обеспечивает успех дальнейшего расследования компьютерных преступлений.

Источник: Сайт **Центра исследования проблем компьютерной преступности**

Лекция 5. Административный уровень информационной безопасности

Основные понятия

К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые руководством организации.

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

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Термин "политика безопасности" является не совсем точным переводом английского словосочетания "security policy", однако в данном случае калька лучше отражает смысл этого понятия, чем лингвистически более верные "правила безопасности". Мы будем иметь в виду не отдельные правила или их наборы (такого рода решения выносятся на процедурный уровень, речь о котором впереди), а стратегию организации в области информационной безопасности. Для выработки стратегии

и проведения ее в жизнь нужны, несомненно, политические решения, принимаемые на самом высоком уровне.

Под политикой безопасности мы будем понимать совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.

Такая трактовка, конечно, гораздо шире, чем набор правил разграничения доступа (именно это означал термин "security policy" в "Оранжевой книге" и в построенных на ее основе нормативных документах других стран).

ИС организации и связанные с ней интересы субъектов - это сложная система, для рассмотрения которой необходимо применять объектно-ориентированный подход и понятие уровня детализации. Целесообразно выделить, по крайней мере, три таких уровня, что мы уже делали в примере и сделаем еще раз далее.

Чтобы рассматривать ИС предметно, с использованием актуальных данных, следует составить карту информационной системы. Эта карта, разумеется, должна быть изготовлена в объектно-ориентированном стиле, с возможностью варьировать не только уровень детализации, но и видимые грани объектов. Техническим средством составления, сопровождения и визуализации подобных карт может служить свободно распространяемый каркас какой-либо системы управления.

Политика безопасности

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К **верхнему уровню** можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации. Примерный список подобных решений может включать в себя следующие элементы:

- решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;
- формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- обеспечение базы для соблюдения законов и правил;
- формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

- вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;
- организационный, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности;
- классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;

- штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п.);
- раздел, освещающий вопросы физической защиты;
- управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;
- раздел, описывающий правила разграничения доступа к производственной информации;
- раздел, характеризующий порядок разработки и сопровождения систем;
- раздел, описывающий меры, направленные на обеспечение непрерывной работы организации;
- юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

К **среднему уровню** можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем. Примеры таких вопросов - отношение к передовым (но, возможно, недостаточно проверенным) технологиям, доступ в Internet (как совместить свободу доступа к информации с защитой от внешних угроз?), использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т.д.

Политика среднего уровня должна для каждого аспекта освещать следующие темы:

Описание аспекта. Например, если рассмотреть применение пользователями неофициального программного обеспечения, последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

Область применения. Следует определить, где, когда, как, по отношению к кому и чему применяется данная политика безопасности. Например, касается ли политика, связанная с использованием неофициального программного обеспечения, организаций-субподрядчиков? Затрагивает ли она сотрудников, пользующихся портативными и домашними компьютерами и вынужденных переносить информацию на производственные машины?

Позиция организации по данному аспекту. Продолжая пример с неофициальным программным обеспечением, можно представить себе позиции полного запрета, выработки процедуры приемки подобного ПО и т.п. Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще стиль документов, определяющих политику безопасности (как и их перечень), в разных организациях может сильно отличаться.

Роли и обязанности. В "политический" документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

Законопослушность. Политика должна содержать общее описание запрещенных действий и наказаний за них.

Точки контакта. Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно "точкой контакта" служит определенное должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам. Она включает в себя два аспекта - цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время, эти вещи настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне. Приведем несколько примеров вопросов, на которые следует дать ответ в политике безопасности нижнего уровня:

- кто имеет право доступа к объектам, поддерживаемым сервисом?
- при каких условиях можно читать и модифицировать данные?
- как организован удаленный доступ к сервису?

При формулировке целей политики нижнего уровня можно исходить из соображений целостности, доступности и конфиденциальности, но нельзя на этом останавливаться. Ее цели должны быть более конкретными. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жесткие правила могут мешать работе пользователей, вероятно, их придется часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уро-

вень безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного вопроса.

Программа безопасности

После того, как сформулирована политика безопасности, можно приступать к составлению программы ее реализации и собственно к реализации.

Чтобы понять и реализовать какую-либо программу, ее нужно структурировать по уровням, обычно в соответствии со структурой организации. В простейшем и самом распространенном случае достаточно двух уровней - верхнего, или центрального, который охватывает всю организацию, и нижнего, или служебного, который относится к отдельным услугам или группам однородных сервисов.

Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. У этой программы следующие главные цели:

- управление рисками (оценка рисков, выбор эффективных средств защиты);
- координация деятельности в области информационной безопасности, пополнение и распределение ресурсов;
- стратегическое планирование;
- контроль деятельности в области информационной безопасности.

В рамках программы верхнего уровня принимаются стратегические решения по обеспечению безопасности, оцениваются технологические новинки. Информационные технологии развиваются очень быстро, и необходимо иметь четкую политику отслеживания и внедрения новых средств.

Контроль деятельности в области безопасности имеет двустороннюю направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат законам. При этом следует поддерживать контакты с внешними контролирующими организациями. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на случаи нарушений и дорабатывать защитные меры с учетом изменения обстановки.

Следует подчеркнуть, что программа верхнего уровня должна занимать строго определенное место в деятельности организации, она должна официально приниматься и поддерживаться руководством, а также иметь определенный штат и бюджет.

Цель программы нижнего уровня - обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие следует использовать механизмы защиты; закупаются и устанавливаются технические средства; выполняется повседневное администрирование; отслеживается состояние слабых мест и т.п. Обычно за программу нижнего уровня отвечают администраторы сервисов.

Синхронизация программы безопасности с жизненным циклом систем

Если синхронизировать программу безопасности нижнего уровня с жизненным циклом защищаемого сервиса, можно добиться большего эффекта с меньшими затратами. Программисты знают, что добавить новую возможность к уже готовой системе на порядок сложнее, чем изначально спроектировать и реализовать ее. То же справедливо и для информационной безопасности.

В жизненном цикле информационного сервиса можно выделить следующие этапы:

Инициация. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.

Закупка. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.

Установка. Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.

Эксплуатация. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

Выведение из эксплуатации. Происходит переход на новый сервис.

Рассмотрим действия, выполняемые на каждом из этапов, более подробно.

На этапе инициации оформляется понимание того, что необходимо приобрести новый или значительно модернизировать существующий сервис; определяется, какими характеристиками и какой функциональностью он должен обладать; оцениваются финансовые и иные ограничения.

С точки зрения безопасности важнейшим действием здесь является оценка критичности как самого сервиса, так и информации, которая с его помощью будет обрабатываться. Требуется сформулировать ответы на следующие вопросы:

- какого рода информация предназначается для обслуживания новым сервисом?
- каковы возможные последствия нарушения конфиденциальности, целостности и доступности этой информации?
- каковы угрозы, по отношению к которым сервис и информация будут наиболее уязвимы?
- есть ли какие-либо особенности нового сервиса (например, территориальная распределенность компонентов), требующие принятия специальных процедурных мер?
- каковы характеристики персонала, имеющие отношение к безопасности (квалификация, благонадежность)?

- каковы законодательные положения и внутренние правила, которым должен соответствовать новый сервис?

Результаты оценки критичности являются отправной точкой в составлении спецификаций. Кроме того, они определяют ту меру внимания, которую служба безопасности организации должна уделять новому сервису на последующих этапах его жизненного цикла.

Этап закупки - один из самых сложных. Нужно окончательно сформулировать требования к защитным средствам нового сервиса, к компании, которая может претендовать на роль поставщика, и к квалификации, которой должен обладать персонал, использующий или обслуживающий закупаемый продукт. Все эти сведения оформляются в виде спецификации, куда входят не только аппаратура и программы, но и документация, обслуживание, обучение персонала. Разумеется, особое внимание должно уделяться вопросам совместимости нового сервиса с существующей конфигурацией. Подчеркнем также, что нередко средства безопасности являются необязательными компонентами коммерческих продуктов, и нужно проследить, чтобы соответствующие пункты не выпали из спецификации.

Когда продукт закуплен, его необходимо установить. Несмотря на кажущуюся простоту, **установка является очень ответственным делом**. Во-первых, новый продукт следует сконфигурировать. Как правило, коммерческие продукты поставляются с отключенными средствами безопасности; их необходимо включить и должным образом настроить. Для большой организации, где много пользователей и данных, начальная настройка может стать весьма трудоемким и ответственным делом.

Во-вторых, новый сервис нуждается в процедурных регуляторах. Следует позаботиться о чистоте и охране помещения, о документах, регламентирующих использование сервиса, о подготовке планов на случай экстренных ситуаций, об организации обучения пользователей и т.п.

После принятия перечисленных мер необходимо провести тестирование. Его полнота и комплексность могут служить гарантией безопасности эксплуатации в штатном режиме.

Период эксплуатации - самый длительный и сложный. С психологической точки зрения наибольшую опасность в это время представляют незначительные изменения в конфигурации сервиса, в поведении пользователей и администраторов. Если безопасность не поддерживать, она ослабевает. Пользователи не столь ревностно выполняют должностные инструкции, администраторы менее тщательно анализируют регистрационную информацию. То один, то другой пользователь получает дополнительные привилегии. Кажется, что в сущности ничего не изменилось; на самом же деле от былой безопасности не осталось и следа.

Для борьбы с эффектом медленных изменений приходится прибегать к периодическим проверкам безопасности сервиса. Разумеется, после значительных модификаций подобные проверки являются обязательными.

При **выведении из эксплуатации** затрагиваются аппаратно-программные компоненты сервиса и обрабатываемые им данные. Аппаратура продается, утилизируется или выбрасывается. Только в специфических случаях необходимо заботиться о физическом разрушении аппаратных компонентов, хранящих конфиденциальную информацию. Программы, вероятно, просто стираются, если иное не предусмотрено лицензионным соглашением.

При выведении данных из эксплуатации их обычно переносят на другую систему, архивируют, выбрасывают или уничтожают. Если архивирование производится с намерением впоследствии прочитать данные в другом месте, следует позаботиться об аппаратно-программной совместимости средств чтения и записи. Информационные технологии развиваются очень быстро, и через несколько лет устройств, способных прочитать старый носитель, может просто не оказаться. Если данные архивируются в зашифрованном виде, необходимо сохранить ключ и средства расшифровки. При архивировании и хранении архивной информации нельзя забывать о поддержании конфиденциальности данных.

Лекция 6. Управление рисками

Основные понятия

Тема управление рисками рассматривается нами на административном уровне ИБ, поскольку только руководство организации способно выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ.

Вообще говоря, **управление рисками, равно как и выработка собственной политики безопасности, нужно только для тех организаций, информационные системы которых и/или обрабатываемые данные можно считать нестандартными.** Типовую организацию вполне устроит типовой набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков (особенно это верно с формальной точки зрения, в свете проанализированного нами ранее российского законодательства в области ИБ). Можно провести аналогию между индивидуальным строительством и получением квартиры в районе массовой застройки. В первом случае необходимо принять множество решений, оформить большое количество бумаг, во втором достаточно определиться лишь с несколькими параметрами. Более подробно данный аспект рассмотрен в статье Сергея Симонова "Анализ рисков, управления рисками" (Jet Info, 1999, 1).

Использование информационных систем связано с определенной совокупностью рисков. Когда риск (возможный ущерб) неприемлемо велик, необходимо принять экономически оправданные защитные меры. Периодическая (пере)оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

С количественной точки зрения размер риска является функцией вероятности реализации определенной угрозы (использующей некоторые уязвимости), а также величины возможного ущерба.

Таким образом, суть работы по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры по уменьшению этого размера и затем убедиться, что риски заключены в приемлемые рамки (и остаются таковыми). Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически:

- (пере)оценку (измерение) рисков;
- выбор эффективных и экономичных защитных средств (нейтрализация рисков).

По отношению к выявленным рискам возможны следующие действия:

- ликвидация риска (например, за счет устранения причины);
- уменьшение риска (например, за счет использования дополнительных защитных средств);
- принятие риска (и выработка плана действия в соответствующих условиях);
- переадресация риска (например, путем заключения страхового соглашения).

Процесс управления рисками можно подразделить на следующие этапы:

(1) выбор анализируемых объектов и уровня детализации их рассмотрения;
(2) выбор методологии оценки рисков;
(3) идентификация активов;
(4) анализ угроз и их последствий, определение уязвимостей в защите;
(5) оценка рисков;
(6) выбор защитных мер;
(7) реализация и проверка выбранных мер;
(8) оценка остаточного риска.

Этапы (6) и (7) относятся к выбору защитных средств (нейтрализации рисков), остальные - к оценке рисков.

Уже перечисление этапов показывает, что управление рисками - процесс циклический. По существу, последний этап - это оператор конца цикла, предписывающий вернуться к началу. Риски нужно контролировать постоянно, периодически проводя их переоценку. Отметим, что добросовестно выполненная и тщательно документированная первая оценка может существенно упростить последующую деятельность.

Управление рисками, как и любую другую деятельность в области информационной безопасности, необходимо интегрировать в жизненный цикл ИС. Тогда эффект оказывается наибольшим, а затраты - минимальными. Ранее мы определили пять этапов жизненного цикла. Кратко опишем, что может дать управление рисками на каждом из них.

На этапе инициации известные риски следует учесть при выработке требований к системе вообще и средствам безопасности в частности.

На этапе закупки (разработки) выявленные риски способны помочь при выборе архитектурных решений, играющих ключевую роль в обеспечении безопасности.

На этапе установки выявленные риски следует учитывать при конфигурировании, тестировании и проверке ранее сформулированных требований, а полный цикл управления рисками должен предшествовать внедрению системы в эксплуатацию.

На этапе эксплуатации управление рисками должно сопровождать все существенные изменение в системе.

При выведении системы из эксплуатации управление рисками помогает убедиться в том, что миграция данных происходит безопасным образом.

Подготовительные этапы управления рисками

В этом разделе будут описаны первые три этапа процесса управления рисками.

Выбор анализируемых объектов и уровня детализации их рассмотрения - первый шаг в оценке рисков. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру; однако, если организации крупная, всеобъемлющая оценка может потребовать неприемлемых затрат времени и сил. В таком случае следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приближенностью итоговой оценки. Если важных сервисов все еще много, выбираются те из них, риски для которых заведомо велики или неизвестны.

Мы уже указывали на целесообразность создания карты информационной системы организации. Для управления рисками подобная карта особенно важна, поскольку она наглядно показывает, какие сервисы выбраны для анализа, а какими было решено пренебречь. Если ИС меняется, а карта поддерживается в актуальном состоянии, то при переоценке рисков сразу станет ясно, какие новые или существенно изменившиеся сервисы нуждаются в рассмотрении.

Вообще говоря, уязвимым является каждый компонент информационной системы - от куска сетевого кабеля, который могут прогрызть мыши, до базы данных, которая может быть разрушена из-за неумелых действий администратора. Как правило, в сферу анализа невозможно включить каждый винтик и каждый байт. Приходится останавливаться на некотором уровне детализации, опять-таки отдавая себе отчет в приближенности оценки. Для новых систем предпочтителен детальный анализ; старая система, подвергшаяся небольшим модификациям, может быть проанализирована более поверхностно.

Очень важно выбрать разумную методологию оценки рисков. Целью оценки является получение ответа на два вопроса: приемлемы ли существующие риски, и если нет, то какие защитные средства экономически целесообразно использовать. Значит, оценка должна быть количественной, допускающей сопоставление с заранее выбранными границами допустимости и расходами на реализацию новых регуляторов безопасности. Управление рисками - типичная оптимизационная задача, и существует довольно много программных продуктов, способных помочь в ее решении (иногда подобные продукты просто прилагаются к книгам по информационной безопасности). Принципиальная трудность, однако, состоит в неточности исходных данных. Можно, конечно, попытаться получить для всех анализируемых величин денежное выражение, высчитать все с точностью до копейки, но большого смысла в этом нет. Практичнее пользоваться условными единицами. В простейшем и вполне допустимом случае можно пользоваться трехбалльной шкалой. Далее мы продемонстрируем, как это делается.

При идентификации активов, то есть тех ресурсов и ценностей, которые организация пытается защитить, следует, конечно, учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, такие как репутация организации. Отправной точкой здесь является представление о миссии организации, то есть о видимых снаружи основных направлениях деятельности, которые желательно (или необходимо) сохранить в любом случае. Выражаясь объектно-ориентированным языком, следует в первую очередь описать внешний интерфейс организации, рассматриваемой как абстрактный объект.

Одним из главных результатов процесса идентификации активов является получение детальной информационной структуры организации и способов ее (структуры) использования. Эти сведения целесообразно нанести на карту ИС в качестве граней соответствующих объектов.

Информационной основой сколько-нибудь крупной организации является сеть, поэтому в число аппаратных активов следует включить компьютеры (серверы, рабочие станции, ПК), периферийные устройства, внешние интерфейсы, кабельное хозяйство, активное сетевое оборудование (мосты, маршрутизаторы и т.п.). К программным активам, вероятно, будут отнесены операционные системы (сетевая, серверные и клиентские), прикладное программное обеспечение, инструментальные средства, средства управления сетью и отдельными системами, Важно зафиксировать, где (в каких узлах сети) хранится программное обеспечение и из каких узлов используется. Третьим видом информационных активов являются данные, которые хранятся, обрабатываются и передаются по сети. Следует классифицировать данные по типам и степени конфиденциальности, выявить места их хранения и обработки, способы доступа к ним. Все это важно для оценки последствий нарушений информационной безопасности.

Управление рисками - процесс далеко не линейный. Практически все его этапы связаны между собой, и по завершении почти любого из них может выявиться необходимость возврата к предыдущему. Так, при идентификации активов может появиться понимание, что выбранные границы анализа следует расширить, а степень детализации - увеличить. Особенно труден первичный анализ, когда многократные возвраты к началу неизбежны.

Подготовительные этапы управления рисками

В этом разделе будут описаны первые три этапа процесса управления рисками.

Выбор анализируемых объектов и уровня детализации их рассмотрения - первый шаг в оценке рисков. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру; однако, если организации крупная, всеобъемлющая оценка может потребовать неприемлемых затрат времени и сил. В таком случае следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приближенностью итоговой оценки. Если важных сервисов все еще много, выбираются те из них, риски для которых заведомо велики или неизвестны.

Мы уже указывали на целесообразность создания карты информационной системы организации. Для управления рисками подобная карта особенно важна, поскольку она наглядно показывает, какие сервисы выбраны для анализа, а какими было решено пренебречь. Если ИС меняется, а карта поддерживается в актуальном состоянии, то при переоценке рисков сразу станет ясно, какие новые или существенно изменившиеся сервисы нуждаются в рассмотрении.

Вообще говоря, уязвимым является каждый компонент информационной системы - от куска сетевого кабеля, который могут прогрызть мыши, до базы данных, которая может быть разрушена из-за неумелых действий администратора. Как правило, в сферу анализа невозможно включить каждый винтик и каждый байт. Приходится останавливаться на некотором уровне детализации, опять-таки отдавая себе отчет в приближенности оценки. Для новых систем предпочтителен детальный анализ; старая система, подвергшаяся небольшим модификациям, может быть проанализирована более поверхностно.

Очень важно выбрать разумную методологию оценки рисков. Целью оценки является получение ответа на два вопроса: приемлемы ли существующие риски, и если нет, то какие защитные средства

экономически целесообразно использовать. Значит, оценка должна быть количественной, допускающей сопоставление с заранее выбранными границами допустимости и расходами на реализацию новых регуляторов безопасности. Управление рисками - типичная оптимизационная задача, и существует довольно много программных продуктов, способных помочь в ее решении (иногда подобные продукты просто прилагаются к книгам по информационной безопасности). Принципиальная трудность, однако, состоит в неточности исходных данных. Можно, конечно, попытаться получить для всех анализируемых величин денежное выражение, высчитать все с точностью до копейки, но большого смысла в этом нет. Практичнее пользоваться условными единицами. В простейшем и вполне допустимом случае можно пользоваться трехбалльной шкалой. Далее мы продемонстрируем, как это делается.

При идентификации активов, то есть тех ресурсов и ценностей, которые организация пытается защитить, следует, конечно, учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, такие как репутация организации. Отправной точкой здесь является представление о миссии организации, то есть о видимых снаружи основных направлениях деятельности, которые желательно (или необходимо) сохранить в любом случае. Выражаясь объектно-ориентированным языком, следует в первую очередь описать внешний интерфейс организации, рассматриваемой как абстрактный объект.

Одним из главных результатов процесса идентификации активов является получение детальной информационной структуры организации и способов ее (структуры) использования. Эти сведения целесообразно нанести на карту ИС в качестве граней соответствующих объектов.

Информационной основой сколько-нибудь крупной организации является сеть, поэтому в число аппаратных активов следует включить компьютеры (серверы, рабочие станции, ПК), периферийные устройства, внешние интерфейсы, кабельное хозяйство, активное сетевое оборудование (мосты, маршрутизаторы и т.п.). К программным активам, вероятно, будут отнесены операционные системы (сетевая, серверные и клиентские), прикладное программное обеспечение, инструментальные средства, средства управления сетью и отдельными системами, Важно зафиксировать, где (в каких узлах сети) хранится программное обеспечение и из каких узлов используется. Третьим видом информационных активов являются данные, которые хранятся, обрабатываются и передаются по сети. Следует классифицировать данные по типам и степени конфиденциальности, выявить места их хранения и обработки, способы доступа к ним. Все это важно для оценки последствий нарушений информационной безопасности.

Управление рисками - процесс далеко не линейный. Практически все его этапы связаны между собой, и по завершении почти любого из них может выявиться необходимость возврата к предыдущему. Так, при идентификации активов может появиться понимание, что выбранные границы анализа следует расширить, а степень детализации - увеличить. Особенно труден первичный анализ, когда многократные возвраты к началу неизбежны.

Основные этапы управления рисками

Этапы, предшествующие анализу угроз, можно считать подготовительными, поскольку, строго говоря, они впрямую не связаны с рисками. Риск появляется там, где есть угрозы.

Краткий перечень наиболее распространенных угроз был рассмотрен нами ранее. К сожалению, на практике угроз гораздо больше, причем далеко не все из них носят компьютерный характер. Так, вполне реальной угрозой является наличие мышей и тараканов в помещениях, занимаемых организацией. Первые могут повредить кабели, вторые вызвать короткое замыкание. Как правило, наличие той или иной угрозы является следствием уязвимостей в защите информационной системы, которые, в свою очередь, объясняются отсутствием некоторых сервисов безопасности или недостатками в реализующих их защитных механизмах. Опасность прогрызания кабелей проистекает не только из наличия мышей, но и из отсутствия или недостаточной прочности защитной оболочки.

Первый шаг в анализе угроз - их идентификация. Анализируемые виды угроз следует выбрать из соображений здравого смысла (оставив вне поля зрения, например, землетрясения, однако не исключая возможности захвата организации террористами), но в пределах выбранных видов провести максимально полное рассмотрение.

Целесообразно выявлять не только сами угрозы, но и источники их возникновения - это поможет в выборе дополнительных средств защиты. Например, нелегальный вход в систему может стать следствием воспроизведения начального диалога, подбора пароля или подключения к сети неавторизованного оборудования. Очевидно, для противодействия каждому из перечисленных способов нелегального входа нужны свои механизмы безопасности.

После идентификации угрозы необходимо оценить вероятность ее осуществления. Допустимо использовать при этом трехбалльную шкалу (низкая (1), средняя (2) и высокая (3) вероятность).

Кроме вероятности осуществления, важен размер потенциального ущерба. Например, пожары бывают нечасто, но ущерб от каждого из них, как правило, велик. Тяжесть ущерба также можно оценить по трехбалльной шкале.

Оценивая тяжесть ущерба, необходимо иметь в виду не только непосредственные расходы на замену оборудования или восстановление информации, но и более отдаленные, такие как подрыв репутации, ослабление позиций на рынке и т.п. Пусть, например, в результате дефектов в управлении доступом к бухгалтерской информации сотрудники получили возможности корректировать данные о собственной заработной плате. Следствием такого состояния дел может стать не только перерасход бюджетных или корпоративных средств, но и полное разложение коллектива, грозящее развалом организации.

Уязвимости обладают свойством притягивать к себе не только злоумышленников, но и сравнительно честных людей. Не всякий устоит перед искушением немного увеличить свою зарплату, если есть уверенность, что это сойдет в рук. Поэтому, оценивая вероятность осуществления угроз, целесообразно исходить не только из среднестатистических данных, но учитывать также специфику конкретных информационных систем. Если в подвале дома, занимаемого организацией, располагается сауна, а сам дом имеет деревянные перекрытия, то вероятность пожара, к сожалению, оказывается существенно выше средней.

После того, как накоплены исходные данные и оценена степень неопределенности, можно переходить к обработке информации, то есть собственно к оценке рисков. Вполне допустимо применить такой простой метод, как умножение вероятности осуществления угрозы на предполагаемый ущерб. Если для вероятности и ущерба использовать трехбалльную шкалу, то возможных произведений будет шесть: 1, 2, 3, 4, 6 и 9. Первые два результата можно отнести к низкому риску, третий и четвертый - к среднему, два последних - к высокому, после чего появляется возможность снова привести их к трехбалльной шкале. По этой шкале и следует оценивать приемлемость рисков. Правда, граничные случаи, когда вычисленная величина совпала с приемлемой, целесообразно рассматривать более тщательно из-за приближенного характера результата.

Если какие-либо риски оказались недопустимо высокими, необходимо их нейтрализовать, реализовав дополнительные защитные меры. Как правило, для ликвидации или нейтрализации уязвимости, сделавшей реальной опасную угрозу, существует несколько механизмов безопасности, отличающихся эффективностью и стоимостью. Например, если велика вероятность нелегального входа в систему, можно приказать пользователям выбирать длинные пароли (скажем, не менее восьми символов), задействовать программу генерации паролей или закупить интегрированную систему аутентификации на основе интеллектуальных карт. Если имеется вероятность умышленного повреждения сервера баз данных, что грозит серьезными последствиями, можно врезать замок в дверь серверной комнаты или поставить около каждого сервера по охраннику.

Оценивая стоимость защитных мер, приходится, разумеется, учитывать не только прямые расходы на закупку оборудования и/или программ, но и расходы на внедрение новинки и, в частности, на обучение и переподготовку персонала. Эту стоимость также можно выразить по трехбалльной шкале и затем сопоставить ее с разностью между вычисленным и приемлемым риском. Если по этому показателю новое средство оказывается экономически выгодным, его можно принять к дальнейшему рассмотрению (подходящих средств, вероятно, будет несколько). Однако, если средство окажется дорогим, его не следует сразу отбрасывать, памятуя о приближенности расчетов.

Выбирая подходящий способ защиты, целесообразно учитывать возможность экранирования одним сервисом безопасности сразу нескольких прикладных сервисов. Так поступили в Массачусетском технологическом институте, защитив несколько тысяч компьютеров сервером аутентификации Kerberos.

Важным обстоятельством является совместимость нового средства со сложившейся организационной и аппаратно-программной структурой, с традициями организации. Меры безопасности, как правило, носят недружественный характер, что может отрицательно сказаться на энтузиазме сотрудников. Порой сохранение духа открытости важнее минимизации материальных потерь. Впрочем, такого рода ориентиры должны быть расставлены в политике безопасности верхнего уровня.

Можно представить себе ситуацию, когда для нейтрализации риска не существует эффективных и приемлемых по цене мер. Например, компания, базирующаяся в сейсмически опасной зоне, не всегда может позволить себе строительство защищенной штаб-квартиры. В таком случае приходится поднимать планку приемлемого риска и переносить центр тяжести на смягчение последствий и выработку планов восстановления после аварий, стихийных бедствий и иных происшествий. Продолжая пример с сейсмоопасностью, можно рекомендовать регулярное тиражирование данных в другой город и овладение средствами восстановления первичной базы данных.

Как и всякую иную деятельность, реализацию и проверку новых регуляторов безопасности следует предварительно распланировать. В плане необходимо учесть наличие финансовых средств, сроки обучения персонала. Нужно составить план тестирования (автономного и комплексного), если речь идет о программно-техническом механизме защиты.

Когда намеченные меры приняты, необходимо проверить их действенность, то есть убедиться, что остаточные риски стали приемлемыми. Если это на самом деле так, значит, все в порядке и можно спокойно намечать дату ближайшей переоценки. В противном случае придется проанализировать допущенные ошибки и провести повторный сеанс управления рисками немедленно.

Лекция 7. Процедурный уровень информационной безопасности

Основные классы мер процедурного уровня

Мы приступаем к рассмотрению мер безопасности, которые ориентированы на людей, а не на технические средства. Именно люди формируют режим информационной безопасности и они же оказываются главной угрозой, поэтому "человеческий фактор" заслуживает первостепенного внимания.

В отечественных организациях накоплен богатый опыт регламентирования и реализации процедурных (организационных) мер, однако проблема состоит в том, что они пришли из докомпьютерного прошлого, поэтому нуждаются в существенном пересмотре.

Следует осознать ту степень зависимости от компьютерной обработки данных, в которую попало современное общество. Без всякого преувеличения, нужна информационная гражданская оборона. Спокойно, без нагнетания страстей, нужно разъяснять обществу не только преимущества, но и опасности, вытекающие из использования информационных технологий. Акцент следует делать не на военной или криминальной стороне дела, а на чисто гражданских аспектах, связанных с поддержанием нормального функционирования аппаратного и программного обеспечения, то есть концентрироваться на вопросах доступности и целостности данных.

На **процедурном уровне** можно выделить следующие классы мер:

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

Перейдем к детальному рассмотрению выделенных классов.

Управление персоналом

Управление персоналом начинается с приема нового сотрудника на работу и даже раньше - с составления описания должности. Уже на этом этапе желательно привлечение специалиста по информационной безопасности для определения компьютерных привилегий, ассоциируемых с должностью. Существует два общих принципа, которые следует иметь в виду:

- разделение обязанностей;
- минимизация привилегий.

Принцип разделения обязанностей предписывает так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс. Например, нежелательна ситуация, когда крупные платежи от имени организации выполняет один человек. Надежнее поручить одному сотруднику оформлять заявки на подобные платежи, а другому - заверять эти заявки. Другой пример - процедурные ограничения действий суперпользователя. Можно искусственно "расщепить" пароль суперпользователя, сообщив первую его часть одному сотруднику, а вторую - другому. Тогда критически важные действия по администрированию ИС они смогут выполнить только вдвоем, что снижает вероятность ошибок и злоупотреблений.

Принцип минимизации привилегий предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа очевидно - уменьшить ущерб от случайных или умышленных некорректных действий пользователей.

Предварительное составление описания должности позволяет оценить ее критичность и спланировать процедуру проверки и отбора кандидатов. Чем критичнее должность, тем тщательнее нужно проверять кандидатов: навести о них справки, быть может, побеседовать с бывшими сослуживцами и т.д. Подобная процедура может быть длительной и дорогой, поэтому нет смысла усложнять ее сверх необходимого. В то же время, неразумно и совсем отказываться от предварительной проверки, рискуя принять на работу человека с уголовным прошлым или с душевными болезнями.

Когда кандидат отобран, он, вероятно, должен пройти **обучение;** по крайней мере, его следует подробно ознакомить со служебными обязанностями, а также с нормами и процедурами информационной безопасности. Желательно, чтобы меры безопасности были им усвоены до вступления в должность и до заведения его системного счета с входным именем, паролем и привилегиями.

С момента заведения системного счета начинается его администрирование, а также протоколирование и анализ действий пользователя. Постепенно изменяется окружение, в котором работает пользователь, его служебные обязанности и т.п. Все это требует соответствующего изменения привилегий. Техническую сложность составляют временные перемещения сотрудника, выполнение им обязанностей взамен лица, ушедшего в отпуск, и иные обстоятельства, когда полномочия нужно сначала дать, а через некоторое время взять обратно. В такие периоды профиль активности пользователя резко меняется, что создает трудности при выявлении подозрительных ситуаций. Определенную аккуратность следует соблюдать и при выдаче новых постоянных полномочий, не забывая изымать старые права доступа.

Ликвидация системного счета пользователя, особенно в случае конфликта между сотрудником и организацией, должна производиться максимально оперативно (в идеале - одновременно с извещением о наказании или увольнении). Возможно и физическое ограничение доступа к рабочему месту. Разумеется, если сотрудник увольняется, у него нужно принять все его компьютерное хозяйство и, в частности, криптографические ключи, если использовались средства шифрования.

К управлению сотрудниками примыкает администрирование лиц, работающих по контракту (например, специалистов фирмы-поставщика, помогающих запустить новую систему). В соответствии с принципом минимизации привилегий, им нужно выделить ровно столько прав, сколько необходимо, и изъять эти права сразу по окончании контракта. Проблема, однако, состоит в том, что на начальном этапе внедрения "внешние" сотрудники будут администрировать "местных", а не наоборот. Здесь на первый план выходит квалификация персонала организации, его способность быстро обучаться, а также оперативное проведение учебных курсов. Важны и принципы выбора деловых партнеров.

Иногда внешние организации принимают на обслуживание и администрирование ответственные компоненты компьютерной системы, например, сетевое оборудование. Нередко администрирование выполняется в удаленном режиме. Вообще говоря, это создает в системе дополнительные уязвимости, которые необходимо компенсировать усиленным контролем средств удаленного доступа или, опять-таки, обучением собственных сотрудников.

Мы видим, что проблема обучения - одна из центральных с точки зрения информационной безопасности. Если сотрудник не знаком с политикой безопасности своей организации, он не может стремиться к достижению сформулированных в ней целей. Если он не знает мер безопасности, он не сможет их соблюдать. Напротив, если сотрудник знает, что его действия протоколируются, он, возможно, воздержится от нарушений.

Физическая защита

Безопасность информационной системы зависит от окружения, в котором она функционирует. Необходимо принять меры для защиты зданий и прилегающей территории, поддерживающей инфраструктуры, вычислительной техники, носителей данных.

Основной принцип физической защиты, соблюдение которого следует постоянно контролировать, формулируется как **"непрерывность защиты в пространстве и времени"**. Ранее мы рассматривали понятие окна уязвимости. Для физической защиты таких окон быть не должно.

Мы кратко рассмотрим следующие направления физической защиты:

- физическое управление доступом;
- противопожарные меры;
- защита поддерживающей инфраструктуры;
- защита от перехвата данных;
- защита мобильных систем.

Меры физического управления доступом позволяют контролировать и при необходимости ограничивать вход и выход сотрудников и посетителей. Контролироваться может все здание организации и, кроме того, отдельные помещения, например, те, где расположены серверы, коммуникационная аппаратура и т.п.

При проектировании и реализации мер физического управления доступом целесообразно применять **объектный подход.** Во-первых, определяется **периметр безопасности,** ограничивающий **контролируемую территорию**. На этом уровне детализации важно продумать внешний интерфейс организации - порядок входа/выхода штатных сотрудников и посетителей, вноса/выноса техники. Все, что не входит во внешний интерфейс, должно быть инкапсулировано, то есть защищено от нелегальных проникновений.

Во-вторых, производится декомпозиция контролируемой территории, выделяются (под)объекты и связи (проходы) между ними. При такой, более глубокой детализации следует произвести приоретизацию подобъектов, выделить среди них наиболее критичные с точки зрения безопасности и обеспечить им повышенное внимание. Декомпозиция должна быть семантически оправданной, обеспечивающей разграничение разнородных сущностей, таких как оборудование разных владельцев или персонал, работающий с данными разной степени критичности. Важно в максимальной степени разграничить компьютеры и поток посетителей или, в крайнем случае, позаботиться о том, чтобы от окон и дверей не просматривались экраны мониторов и принтеры. Необходимо, чтобы посетители отличались от штатных сотрудников. Если отличие состоит в том, что посетителям выдаются идентификационные карточки, а сотрудники ходят "без опознавательных знаков", злоумышленнику достаточно снять карточку, чтобы его считали "своим". Очевидно, карточки разных видов нужны всем.

Средства физического управления доступом известны давно. Это охрана, двери с замками, перегородки, телекамеры, датчики движения и многое другое. Для выбора оптимального (по критерию стоимость/эффективность) средства целесообразно провести анализ рисков (к этому соображению мы еще вернемся). Кроме того, есть смысл периодически отслеживать появление технических новинок в данной области, стремясь к максимальной автоматизации физической защиты.

Более подробно данная тема рассмотрена в статье В. Барсукова "Физическая защита информационных систем" (Jet Info, 1997, 1).

Профессия пожарника - одна из древнейших, но пожары по-прежнему случаются и наносят большой ущерб. Мы не собираемся цитировать параграфы противопожарных инструкций или изобретать новые методы борьбы с огнем - для этого есть профессионалы. Отметим лишь крайнюю желательность установки противопожарной сигнализации и автоматических средств пожаротушения. Обратим также внимание на то, как защитные меры могут создавать новые слабости. Если на работу взят новый охранник, это, вероятно, улучшает физическое управление доступом. Если же он по ночам курит и пьет, то повышенная пожарная опасность делает его скорее врагом, чем другом организации.

К поддерживающей инфраструктуре можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций. В принципе, к ним применимы те же требования целостности и доступности, что и к информационным системам. Для обеспечения целостности нужно защищать оборудование от краж и повреждений. Для поддержания доступности целесообразно выбирать оборудование с максимальным временем наработки на отказ, дублировать ответственные узлы, всегда иметь под рукой запчасти.

Отдельную проблему составляют аварии водопровода. Они происходят нечасто, но чреваты серьезными материальными потерями. При размещении компьютеров разумно принять во внимание расположение водопроводных и канализационных труб и постараться держаться от них подальше. Сотрудники должны знать, куда следует обращаться при обнаружении протечек.

Перехват данных (о чем мы уже писали) может осуществляться самыми разными способами: подсматриванием за экраном монитора, чтением пакетов, передаваемых по сети, анализом побочных электромагнитных излучений и наводок (ПЭМИН) и т.д. Остается уповать на повсеместное использование криптографии (что, впрочем, сопряжено у нас в стране со множеством технических и законодательных проблем), стараться в максимально возможной степени расширить контролируемую территорию, разместившись в тихом особняке, поодаль от других домов, пытаться держать под контролем линии связи (например, заключать их в надувную оболочку с обнаружением прокалывания), но главное, вероятно, состоит в том, что нужно по возможности избавиться от паранойи и осознать, что для коммерческих систем обеспечение конфиденциальности не является главной задачей.

Желающим подробнее ознакомиться с данной тематикой мы рекомендуем статью В. Барсукова "Блокирование технологических каналов утечки информации" (Jet Info, 1998, 5-6).

Мобильные и портативные компьютеры - заманчивый объект кражи. Их довольно часто оставляют без присмотра, в автомобиле или на работе, и унести и спрятать такой компьютер весьма несложно. Довольно часто средства массовой информации сообщают о том, что какой-нибудь офицер английской разведки или американский военный лишился таким образом движимого имущества. Следует настоятельно рекомендовать шифрование данных на жестких дисках подобных компьютеров.

Вообще говоря, при выборе средств физической защиты следует производить анализ рисков. Так, принимая решение о закупке источника бесперебойного питания, необходимо учесть качество электропитания в здании, занимаемом организацией (впрочем, почти наверняка оно окажется плохим), характер и длительность нарушений питания, стоимость доступных источников и возможные потери от аварий (выход из строя техники, приостановка работы организации и т.п.) (см. также статью В. Барсукова "Защита компьютерных систем от силовых деструктивных воздействий" в Jet Info, 2000, 2). В то же время, во многих случаях решения очевидны. Меры противопожарной безопасности обязательны для всех организаций. Стоимость реализации многих мер (например, установка обычного замка на дверь серверной комнаты) пренебрежимо мала, другие имеют хоть и заметную стоимость, но все же явно меньшую, чем возможный ущерб. К числу последних можно отнести регулярное копирование больших баз данных. Физическая защита, как и другие области информационной безопасности, должна базироваться на здравом смысле, который подскажет большинство решений.

Поддержание работоспособности

Мы переходим к рассмотрению рутинных действий, направленных на поддержание работоспособности информационных систем. Именно здесь таится наибольшая опасность. Нечаянные ошибки системных администраторов и пользователей грозят повреждением аппаратуры, разрушением программ и данных; "в лучшем случае" создаются уязвимости, делающие возможной реализацию угроз.

Недооценка факторов безопасности в повседневной работе - ахиллесова пята многих организаций. Дорогие средства безопасности теряют смысл, если они плохо документированы, конфликтуют с другим программным обеспечением, а пароль системного администратора не менялся с момента установки.

Можно выделить следующие направления повседневной деятельности:

- поддержка пользователей;
- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;

- документирование;
- регламентные работы.

Поддержка пользователей состоит прежде всего в консультировании и в оказании помощи при решении разного рода проблем. Иногда в организациях создают для этой цели специальный "стол справок"; чаще от пользователей отбивается системный администратор. Очень важно в потоке вопросов, умных и не очень, уметь выявлять проблемы, связанные с информационной безопасностью. Так, многие трудности пользователей, работающих на персональных компьютерах, могут быть следствием заражения вирусами. Целесообразно фиксировать вопросы пользователей, чтобы выявлять их типичные ошибки и выпускать памятки с рекомендациями для распространенных ситуаций.

Поддержка программного обеспечения - одно из важнейших средств обеспечения целостности информации. Прежде всего, необходимо контролировать, какое программное обеспечение выполняется на компьютерах. Если пользователи могут устанавливать программы по своему усмотрению, это чревато заражением вирусами, а также появлением утилит, действующих в обход защитных средств. Вполне вероятно также, что самодеятельность пользователей постепенно приведет к хаосу на их компьютерах, а исправлять ситуацию придется системному администратору.

Второй аспект поддержки программного обеспечения - контроль за отсутствием неавторизованного изменения программ и прав доступа к ним. Сюда же можно отнести поддержание эталонных копий программных систем. Обычно контроль достигается комбинированием средств физического и логического управления доступом, а также использованием утилит проверки и поддержания целостности.

Конфигурационное управление позволяет контролировать и фиксировать изменения, вносимые в программную конфигурацию. Прежде всего, необходимо застраховаться от случайных или непродуманных модификаций, уметь как минимум возвращаться к прошлой, работающей версии. Фиксация изменений позволит легко восстановить текущую версию после аварии.

Лучший способ уменьшить количество ошибок в рутинной работе - в максимальной степени автоматизировать ее. Правы "ленивые" программисты и системные администраторы, которые, поглядев на море однообразных задач, говорят: "Я ни за что не буду делать этого; я напишу программу, которая сделает все за меня". **Автоматизация и безопасность - родные сестры; тот, кто заботится в первую очередь об облегчении собственного труда, на самом деле оптимальным образом формирует режим информационной безопасности.**

Резервное копирование необходимо для восстановления программ и данных после аварий. И здесь целесообразно автоматизировать работу, как минимум сформировав компьютерное расписание выполнения полных и инкрементальных копий, а как максимум воспользовавшись соответствующими программными продуктами (см., например, Jet Info, 2000, 12). Нужно также наладить размещение копий в безопасном месте, защищенном от несанкционированного доступа, пожаров, протечек, то есть от всего, что чревато кражей или повреждением носителей. Целесообразно иметь несколько экземпляров резервных копий и часть из них хранить вне территории организации, защищаясь таким образом от крупных аварий и аналогичных инцидентов.

Время от времени в тестовых целях следует проверять возможность восстановления информации с копий.

Управление носителями служит для обеспечения физической защиты и учета дискет, лент, печатных выдач и т.п. Управление носителями должно обеспечить конфиденциальность, целостность и доступность информации, хранящейся вне компьютерных систем. Под физической защитой здесь понимается не только отражение попыток несанкционированного доступа, но и предохранение от вредных влияний окружающей среды (жары, холода, влаги, магнетизма). Управление носителями должно охватывать весь жизненный цикл - от закупки до выведения из эксплуатации.

Документирование - неотъемлемая часть информационной безопасности. В виде документов оформляется почти все - от политики безопасности до журнала учета носителей. Важно, чтобы документация была актуальной, отражала текущее, а не прошлое, состояние дел, причем отражала в непротиворечивом виде.

К хранению некоторых документов (содержащих, например, анализ системных уязвимостей и угроз) применимы требования обеспечения конфиденциальности, к другим, таким как план восстановления после аварий - требования целостности и доступности (в критической ситуации план необходимо найти и прочитать).

Регламентные работы - очень серьезная угроза безопасности. Лицо, осуществляющее регламентные работы, получает исключительный доступ к системе, и на практике очень трудно проконтролировать, какие именно действия совершаются. Здесь на первый план выходит степень доверия к тем, кто выполняет работы.

Реагирование на нарушения режима безопасности

Программа безопасности, принятая организацией, должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима информационной безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.

Реакция на нарушения режима безопасности преследует три главные цели:

- локализация инцидента и уменьшение наносимого вреда;
- прослеживание нарушителя;
- недопущение повторных нарушений.

В организации должен быть человек, доступный 24 часа в сутки (лично, по телефону, пейджеру или электронной почте), отвечающий за реакцию на нарушения. Все должны знать координаты этого человека и обращаться к нему при первых признаках опасности. В общем, нужно действовать, как при пожаре: знать, куда звонить, и что делать до приезда пожарной команды.

Важность быстрой и скоординированной реакции можно продемонстрировать на следующем примере. Пусть локальная сеть предприятия состоит из двух сегментов, администрируемых разными людьми. Пусть, далее, в один из сегментов был внесен вирус. Почти наверняка через несколько минут (или, в крайнем случае, несколько десятков минут) вирус распространится и на другой сегмент. Значит, меры нужны немедленные. Далее, вычищать вирус нужно одновременно в обоих сегментах; в противном случае сегмент, вычищенный первым, заразится от другого, а затем вирус вернется и во второй сегмент.

Нередко требование локализации инцидента и уменьшения наносимого вреда вступает в конфликт с желанием проследить нарушителя. В политике безопасности организации должны быть заранее расставлены приоритеты. Поскольку, как показывает практика, на успешное прослеживание не так уж много шансов, на наш взгляд, в первую очередь следует заботиться об уменьшении ущерба.

Для прослеживания нарушителя нужно заранее выяснить контактные координаты поставщика сетевых услуг и договориться с ним о самой возможности и порядке выполнения соответствующих действий. Более подробно данная тема освещена в статье Н. Браунли и Э. Гатмэна "Как реагировать на нарушения информационной безопасности (RFC 2350, BCP 21)" (Jet Info, 2000, 5).

Для недопущения повторных нарушений необходимо анализировать каждый инцидент, выявлять причины, накапливать статистику. Каковы источники вредоносного ПО? Какие пользователи имеют обыкновение выбирать слабые пароли? На подобные вопросы и должны дать ответ результаты анализа.

Необходимо **отслеживать появление новых уязвимостей** и как можно оперативнее ликвидировать ассоциированные с ними окна опасности. Кто-то в организации должен курировать этот процесс, принимать краткосрочные меры и корректировать программу безопасности для принятия долгосрочных мер.

Планирование восстановительных работ

Ни одна организация не застрахована от серьезных аварий, вызванных естественными причинами, чьим-то злым умыслом, халатностью или некомпетентностью. В то же время, у каждой организации есть **функции**, которые она считает **критически** важными, выполнение которых она хотела бы продолжать, несмотря ни на что. Планирование восстановительных работ позволяет подготовиться к авариям, уменьшить ущерб от них и сохранить способность к функционированию хотя бы в минимальном объеме.

Отметим, что меры информационной безопасности можно разделить на три группы, в соответствии с тем, направлены ли они на предупреждение, обнаружение или ликвидацию последствий атак. Большинство мер носят предупредительный характер. Оперативный анализ регистрационной информации и некоторые аспекты реагирования на нарушения (так называемый активный аудит) служат для обнаружения и отражения атак. Планирование восстановительных работ, очевидно, можно отнести к последней из трех перечисленных групп.

Процесс планирования восстановительных работ можно подразделить на следующие этапы:

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

Планируя восстановительные работы, следует отдавать себе отчет в том, что полностью сохранить функционирование организации не всегда возможно. Необходимо выявить критически важные функции, без которых организация теряет свое лицо, и даже среди критичных функций расставить приоритеты, чтобы как можно быстрее и с минимальными затратами возобновить деятельность после аварии.

Идентифицируя ресурсы, необходимые для выполнения критически важных функций, следует помнить, что многие из них имеют некомпьютерный характер. На этом этапе желательно привлечение специалистов разного профиля, способных в совокупности охватить все аспекты проблемы. Критичные ресурсы обычно относятся к одной из следующих категорий:

- персонал,
- информационная инфраструктура,
- физическая инфраструктура.

Составляя списки критически важных специалистов, следует учитывать, что некоторые из них могут впрямую пострадать от аварии (например, от пожара), кто-то может находиться в состоянии стресса, часть сотрудников, возможно, будет лишена возможности попасть на работу (например, в случае массовых беспорядков). Желательно иметь некоторый резерв специалистов или заранее определить каналы, по которым можно на время привлечь дополнительный персонал.

Информационная инфраструктура включает в себя следующие элементы:

- компьютеры,
- программы и данные,
- информационные сервисы внешних организаций,
- документацию.

Нужно подготовиться к тому, что на "запасном аэродроме", куда организация будет эвакуирована после аварии, аппаратная платформа может отличаться от исходной. Соответственно, следует продумать меры поддержания совместимости по программам и данным.

Среди внешних информационных сервисов для коммерческих организаций, вероятно, важнее всего получение оперативной информации и связь с государственными службами, курирующими данный сектор экономики.

Документация важна хотя бы потому, что не вся информация, с которой оперирует организация, представлена в электронной форме. Скорее всего, план восстановительных работ напечатан на бумаге.

К физической инфраструктуре относятся здания, инженерные коммуникации, средства связи, оргтехника и многое другое. Компьютерная техника не может работать в плохих условиях, без нормального электропитания и т.п.

Анализируя критичные ресурсы, целесообразно учесть временной профиль их использования. Большинство ресурсов нужны постоянно, но в некоторых нужда может возникать только в определенные периоды (например, в конце месяца или года при составлении отчета).

При определении перечня возможных аварий нужно попытаться разработать их сценарии. Как будут развиваться события? Каковы могут оказаться масштабы бедствия? Что произойдет с критичными ресурсами? Например, смогут ли люди попасть на работу? Будут ли выведены из строя компьютеры? Возможны ли случаи саботажа? Будет ли работать связь? Пострадает ли здание организации? Можно ли будет найти и прочитать необходимые бумаги?

Стратегия восстановительных работ должна базироваться на наличных ресурсах и быть не слишком накладной для организации. При разработке стратегии целесообразно провести анализ рисков, которым подвержены критичные функции, и попытаться выбрать наиболее экономичное решение.

Стратегия должна предусматривать не только работу по временной схеме, но и возвращение к нормальному функционированию.

Подготовка к реализации выбранной стратегии состоит в проработке детального плана действий в экстренных ситуациях и по их окончании, а также в обеспечении некоторой избыточности критичных ресурсов. Последнюю цель можно достичь без большого расхода средств, если заключить с одной или несколькими организациями соглашения о взаимной поддержке в случае аварий - тот, кто не пострадал, предоставляют часть своих ресурсов во временное пользование менее удачливым партнерам.

Избыточность обеспечивается также мерами резервного копирования, хранением копий в нескольких местах, представлением информации в разных видах (на бумаге и в файлах) и т.д.

Разумно заключить соглашение с поставщиками информационных услуг о первоочередном обслуживании в критических ситуациях или иметь соглашения с несколькими поставщиками. Правда, эти меры могут потребовать определенных расходов.

Проверка стратегии производится путем анализа подготовленного плана, принятых и намеченных мер.

Лекция 8. Основные программно-технические меры

Основные понятия программно-технического уровня информационной безопасности

Программно-технические меры, то есть меры, направленные на контроль компьютерных сущностей - оборудования, программ и/или данных, образуют последний и самый важный рубеж информационной безопасности. Напомним, что основную часть ущерба наносят действия легальных пользователей, по отношению к которым процедурные регуляторы не могут дать решающего эффекта. Главные враги - некомпетентность и неаккуратность при выполнении служебных обязанностей, и только программно-технические меры способны им противостоять.

Компьютеры помогли автоматизировать многие области человеческой деятельности. Вполне естественным представляется желание возложить на них и обеспечение собственной безопасности. Даже физическую защиту все чаще поручают не охранникам, а интегрированным компьютерным системам, что позволяет одновременно отслеживать перемещения сотрудников и по пространству

организации, и по информационному пространству. Это вторая причина, объясняющая важность программно-технических мер.

Следует, однако, учитывать, что быстрое развитие информационных технологий не только дает новые возможности обороняющимся, но и объективно затрудняет обеспечение надежной защиты, если опираться исключительно на меры программно-технического уровня. Причин тому несколько:

- повышение быстродействия микросхем, развитие архитектур с высокой степенью параллелизма позволяет методом грубой силы преодолевать барьеры (прежде всего криптографические), ранее казавшиеся неприступными;
- развитие сетей и сетевых технологий, увеличение числа связей между информационными системами, рост пропускной способности каналов расширяют число злоумышленников, имеющих техническую возможность организовывать атаки;
- появление новых информационных сервисов ведет и к появлению новых уязвимостей как "внутри" сервисов, так и на их стыках;
- конкуренция среди производителей программного обеспечения заставляет сокращать сроки разработки, что ведет к снижению качества тестирования и выпуску продуктов с дефектами защиты;
- навязываемая потребителям парадигма постоянного наращивания аппаратного и программного обеспечения не позволяет долго оставаться в рамках надежных, апробированных конфигураций и, кроме того, вступает в конфликт с бюджетными ограничениями, из-за чего снижается доля ассигнований на безопасность.
- Перечисленные соображения лишний раз подчеркивают важность комплексного подхода к информационной безопасности, а также необходимость динамичной позиции при выборе и сопровождении программно-технических регуляторов.

Центральным для программно-технического уровня является понятие **сервиса безопасности.**

Следуя объектно-ориентированному подходу, при рассмотрении информационной системы с единичным уровнем детализации мы увидим совокупность предоставляемых ею информационных сервисов. Назовем их основными. Чтобы они могли функционировать и обладали требуемыми свойствами, необходимо несколько уровней дополнительных (вспомогательных) сервисов - от СУБД и мониторов транзакций до ядра операционной системы и оборудования.

В число вспомогательных входят сервисы безопасности (мы уже сталкивались с ними при рассмотрении стандартов и спецификаций в области ИБ); среди них нас в первую очередь будут интересовать универсальные, высокоуровневые, допускающие использование различными **основными и вспомогательными сервиса**ми. Далее будут изучены:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- шифрование;
- контроль целостности;
- экранирование;
- анализ защищенности;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелирование;
- управление.

Будут описаны требования к сервисам безопасности, их функциональность, возможные методы реализации, место в общей архитектуре.

Если сопоставить приведенный перечень сервисов с классами функциональных требований "Общих критериев", то бросается в глаза их существенное несовпадение. Мы отказались от рассмотрения вопросов, связанных с **приватностью**, по следующей причине. На наш взгляд, сервис безопасности, хотя бы частично, должен находиться в распоряжении того, кого он защищает. В ситуации с приватностью это не так: критически важные компоненты сосредоточены не на клиентской, а на серверной стороне, так что приватность по существу оказывается свойством предлагаемой информационной услуги (в простейшем случае приватность достигается сохранением конфиденциальности серверной регистрационной информации и защитой от перехвата данных, для чего достаточно перечисленных нами сервисов безопасности).

С другой стороны, наш перечень шире, чем в "Общих критериях", поскольку в него входят экранирование, анализ защищенности и туннелирование. Мы покажем, что эти сервисы имеют важное самостоятельное значение и, кроме того, могут комбинироваться с другими сервисами для получения таких необходимых **защитных средств**, как, например, виртуальные собственные сети.

Совокупность перечисленных выше сервисов безопасности мы будем называть полным набором. Согласно современным воззрениям, он в принципе достаточен для построения надежной защиты на программно-техническом уровне, правда, при соблюдении целого ряда дополнительных условий (отсутствие уязвимостей, безопасное администрирование и т.д., и т.п.).

Для проведения классификации сервисов безопасности и определения их места в общей архитектуре целесообразно подразделить меры безопасности на следующие виды:

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

Большинство сервисов безопасности попадает в число превентивных, и это, безусловно, правильно. Аудит и контроль целостности способны помочь в обнаружении нарушений; активный аудит, кроме того, позволяет запрограммировать реакцию на нарушение с целью локализации и/или прослеживания. Направленность сервисов отказоустойчивости и безопасного восстановления очевидна. Наконец, управление играет инфраструктурную роль, обслуживая все аспекты ИС.

Особенности современных информационных систем, существенные с точки зрения безопасности

Информационная система типичной современной организации является весьма сложным образованием, построенным в многоуровневой архитектуре клиент/сервер, пользующимся многочисленными внешними сервисами и, в свою очередь, предоставляющим собственные сервисы вовне. Даже сравнительно небольшие магазины, обеспечивающие расчет с покупателями по пластиковым картам (и, конечно, имеющие внешний Web-**сервер**), критическим образом зависят от своих информационных систем и, в частности (и вместе с покупателями), - от защищенности всех компонентов систем и коммуникаций между ними.

С точки зрения безопасности наиболее существенными представляются следующие аспекты современных ИС:

- корпоративная сеть имеет несколько территориально разнесенных частей (поскольку организация располагается на нескольких производственных площадках), связи между которыми находятся в ведении внешнего поставщика сетевых услуг, выходя за пределы зоны, контролируемой организацией;
- корпоративная сеть имеет одно или несколько подключений к Интернет;
- на каждой из производственных площадок могут находиться критически важные серверы, в доступе к которым нуждаются работники, базирующиеся на других площадках, мобильные работники и, возможно, сотрудники сторонних организаций и другие внешние пользователи;
- для доступа пользователей могут применяться не только компьютеры, но и потребительские устройства, использующие, в частности, беспроводную связь;
- в течение одного сеанса работы пользователю приходится обращаться к нескольким информационным сервисам, опирающимся на разные аппаратно-программные платформы;
- к доступности информационных сервисов предъявляются жесткие требования, обычно выражающиеся в необходимости круглосуточного функционирования с максимальным временем простоя порядка минут или десятков минут;
- информационная система представляет собой сеть с активными агентами, то есть в процессе работы программные компоненты, такие как аплеты или сервлеты, передаются с одной машины на другую и выполняются в целевой среде, поддерживая связь с удаленными компонентами;
- не все пользовательские системы контролируются сетевыми и/или системными администраторами организации;
- программное обеспечение, особенно полученное по сети, не может считаться доверенным, в нем могут присутствовать зловредные элементы или ошибки, создающие уязвимости в защите;
- конфигурация информационной системы постоянно изменяется на уровнях административных данных, программ и аппаратуры (меняется состав пользователей, их привилегии, версии программ, появляются новые сервисы, новая аппаратура и т.п.).

Следует учитывать еще по крайней мере два момента. Во-первых, для каждого сервиса основные грани ИБ (доступность, целостность, конфиденциальность) трактуются по-своему. Целостность с точки зрения системы управления базами данных и с точки зрения почтового сервера - вещи принципиально разные. Бессмысленно говорить о безопасности локальной или иной сети вообще, если сеть включает в себя разнородные компоненты. Следует анализировать защищенность сервисов, функционирующих в сети. Для разных сервисов и защиту строят по-разному. Во-вторых, основная угроза информационной безопасности организаций по-прежнему исходит не от внешних злоумышленников, а от собственных сотрудников, по той или иной причине не являющихся лояльными.

В силу изложенных причин далее будут рассматриваться распределенные, разнородные, многосервисные, эволюционирующие системы. Соответственно, нас будут интересовать решения, ориентированные на подобные конфигурации.

Архитектурная безопасность

Сервисы безопасности, какими бы мощными и стойкими они ни были, сами по себе не могут гарантировать надежность программно-технического уровня защиты. Только разумная, проверенная архитектура способна сделать эффективным объединение сервисов, обеспечить управляемость информационной системы, ее способность развиваться и противостоять новым угрозам при сохранении таких свойств, как высокая производительность, простота и удобство использования.

Теоретической основой решения проблемы архитектурной безопасности является следующее фундаментальное утверждение, которое мы уже приводили при рассмотрении Интерпретации "Оранжевой книги" для сетевых конфигураций:

Утверждение. Пусть каждый субъект (то есть процесс, действующий от имени какого-либо пользователя) заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента. Пусть, далее, каждый компонент содержит свой монитор обращений, отслеживающий все локальные попытки доступа, и все мониторы проводят в жизнь согласованную политику безопасности. Пусть, наконец, коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации. Тогда совокупность всех мониторов образует единый монитор обращений для всей сетевой конфигурации.

Обратим внимание на три принципа, содержащиеся в приведенном утверждении:

- необходимость выработки и проведения в жизнь единой политики безопасности;
- необходимость обеспечения конфиденциальности и целостности при сетевых взаимодействиях;
- необходимость формирования составных сервисов по содержательному принципу, чтобы каждый полученный таким образом компонент обладал полным набором защитных средств и с внешней точки зрения представлял собой единое целое (не должно быть информационных потоков, идущих к незащищенным сервисам).

Если какой-либо (составной) сервис не обладает полным набором защитных средств (состав полного набора описан выше), необходимо привлечение дополнительных сервисов, которые мы будем называть экранирующими. Экранирующие сервисы устанавливаются на путях доступа к недостаточно защищенным элементам; в принципе, один такой сервис может экранировать (защищать) сколь угодно большое число элементов.

С практической точки зрения наиболее важными являются следующие принципы архитектурной безопасности:

- непрерывность защиты в пространстве и времени, невозможность миновать защитные средства;
- следование признанным стандартам, использование апробированных решений;
- иерархическая организация ИС с небольшим числом сущностей на каждом уровне;
- усиление самого слабого звена;
- невозможность перехода в небезопасное состояние;
- минимизация привилегий;
- разделение обязанностей;
- эшелонированность обороны;
- разнообразие защитных средств;
- простота и управляемость информационной системы.
- Поясним смысл перечисленных принципов.

Если у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, он, разумеется, так и сделает. Определенные выше экранирующие сервисы должны исключить подобную возможность.

Следование признанным стандартам, использование апробированных решений повышает надежность ИС, уменьшает вероятность попадания в тупиковую ситуацию, когда обеспечение безопасности потребует непомерно больших затрат и принципиальных модификаций.

Иерархическая организация ИС с небольшим числом сущностей на каждом уровне необходима по технологическим соображениям. При нарушении данного принципа система станет необозримой и, следовательно, обеспечить ее безопасность будет невозможно.

Надежность любой обороны определяется самым слабым звеном. Злоумышленник не будет бороться против силы, он предпочтет легкую победу над слабостью. (Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.)

Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если в крепости механизм подъемного моста ломается, мост должен оставаться в поднятом состоянии, препятствуя проходу неприятеля.

Применительно к программно-техническому уровню принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа - уменьшить ущерб от случайных или умышленных некорректных действий пользователей и администраторов.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, чтобы один человек не мог нарушить критически важный для организации процесс или создать брешь в защите по заказу злоумышленников. Соблюдение данного принципа особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией - управление доступом и, как последний рубеж, - протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками (например, умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

Очень важен принцип простоты и управляемости информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации различных компонентов и осуществить централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (например, таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и плохо управляемой.

Для обеспечения высокой доступности (непрерывности функционирования) необходимо соблюдать следующие принципы архитектурной безопасности:

- Внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т.п.).
- Наличие средств обнаружения нештатных ситуаций.
- Наличие средств реконфигурирования для восстановления, изоляции и/или замены компонентов, отказавших или подвергшихся атаке на доступность.
- Рассредоточенность сетевого управления, отсутствие единой точки отказа.
- Выделение подсетей и изоляция групп пользователей друг от друга. Данная мера, являющаяся обобщением разделения процессов на уровне операционной системы, ограничивает зону поражения при возможных нарушениях информационной безопасности.
- Еще одним важным архитектурным принципом следует признать минимизацию объема защитных средств, выносимых на клиентские системы. Причин тому несколько:
- для доступа в корпоративную сеть могут использовать потребительские устройства с ограниченной функциональностью;
- конфигурацию клиентских систем трудно или невозможно контролировать.

К необходимому минимуму следует отнести реализацию сервисов безопасности на сетевом и транспортном уровнях и поддержку механизмов аутентификации, устойчивых к сетевым угрозам.

Лекция 9. Идентификация и аутентификация, управление доступом

Идентификация и аутентификация. Основные понятия.

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. Идентификация и аутентификация - это первая линия обороны, "проходная" информационного пространства организации.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "аутентификация" иногда используют словосочетание "проверка подлинности".

(Заметим в скобках, что происхождение русскоязычного термина "аутентификация" не совсем понятно. Английское "authentication" скорее можно прочитать как "аутентикация"; трудно сказать, откуда в середине взялось еще "фи" - может, из идентификации? Тем не менее, термин устоялся, он закреплен в Руководящих документах Гостехкомиссии России, использован в многочисленных публикациях, поэтому исправить его уже невозможно.)

Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и **двусторонней (взаимной)**. Пример односторонней аутентификации - процедура входа пользователя в систему.

В сетевой среде, когда стороны идентификации/аутентификации территориально разнесены, у рассматриваемого сервиса есть два основных аспекта:

- что служит аутентификатором (то есть используется для подтверждения подлинности субъекта);
- как организован (и защищен) обмен данными идентификации/аутентификации.
- Субъект может подтвердить свою подлинность, предъявив по крайней мере одну из следующих сущностей:
- нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);
- нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);
- нечто, что есть часть его самого (голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики).

В открытой сетевой среде между сторонами идентификации/аутентификации не существует доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от **перехвата**, **изменения** и/или **воспроизведения** данных. Передача паролей в открытом виде, очевидно, неудовлетворительна; не спасает положение и шифрование паролей, так как оно не защищает от воспроизведения. Нужны более сложные протоколы аутентификации.

Надежная идентификация и аутентификация затруднена не только из-за сетевых угроз, но и по целому ряду причин. Во-первых, почти все аутентификационные сущности можно узнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных. В-третьих, чем надежнее средство защиты, тем оно дороже.

Современные средства идентификации/аутентификации должны поддерживать концепцию единого входа в сеть. **Единый вход в сеть** - это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации.

Любопытно отметить, что сервис идентификации/аутентификации может стать объектом атак на доступность. Если система сконфигурирована так, что после определенного числа неудачных попыток устройство ввода идентификационной информации (такое, например, как терминал) блокируется, то злоумышленник может остановить работу легального пользователя буквально несколькими нажатиями клавиш.

Парольная аутентификация

Главное достоинство **парольной аутентификации** - простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Чтобы пароль был запоминающимся, его зачастую делают простым (имя подруги, название спортивной команды и т.п.). Однако простой пароль нетрудно угадать, особенно если знать пристрастия данного пользователя. Известна классическая история про советского разведчика Рихарда Зорге, объект внимания которого через слово говорил "карамба"; разумеется, этим же словом открывался сверхсекретный сейф.

Иногда пароли с самого начала не хранятся в тайне, так как имеют стандартные значения, указанные в документации, и далеко не всегда после установки системы производится их смена.

Ввод пароля можно подсмотреть. Иногда для подглядывания используются даже оптические приборы.

Пароли нередко сообщают коллегам, чтобы те могли, например, подменить на некоторое время владельца пароля. Теоретически в подобных случаях более правильно задействовать средства управления доступом, но на практике так никто не поступает; а тайна, которую знают двое, это уже не тайна.

Пароль можно угадать "методом грубой силы", используя, скажем, словарь. Если файл паролей зашифрован, но доступен для чтения, его можно скачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор (предполагается, что алгоритм шифрования известен).

Тем не менее, следующие меры позволяют значительно повысить надежность парольной защиты:

- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
- управление сроком действия паролей, их периодическая смена;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему (это затруднит применение "метода грубой силы");
- обучение пользователей;
- использование программных генераторов паролей (такая программа, основываясь на несложных правилах, может порождать только благозвучные и, следовательно, запоминающиеся пароли).

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации.

Одноразовые пароли

Рассмотренные выше пароли можно назвать многоразовыми; их раскрытие позволяет злоумышленнику действовать от имени легального пользователя. Гораздо более сильным средством, устойчивым к пассивному прослушиванию сети, являются одноразовые пароли.

Наиболее известным программным генератором одноразовых паролей является система S/KEY компании Bellcore. Идея этой системы состоит в следующем. Пусть имеется односторонняя функция f (то есть функция, вычислить обратную которой за приемлемое время не представляется возможным). Эта функция известна и пользователю, и серверу аутентификации. Пусть, далее, имеется секретный ключ K, известный только пользователю.

На этапе начального администрирования пользователя функция f применяется к ключу K n раз, после чего результат сохраняется на сервере. После этого процедура проверки подлинности пользователя выглядит следующим образом:

- сервер присылает на пользовательскую систему число (n-1);
- пользователь применяет функцию f к секретному ключу K (n-1) раз и отправляет результат по сети на сервер аутентификации;
- сервер применяет функцию f к полученному от пользователя значению и сравнивает результат с ранее сохраненной величиной. В случае совпадения подлинность пользователя считается установленной, сервер запоминает новое значение (присланное пользователем) и уменьшает на единицу счетчик (n).

На самом деле реализация устроена чуть сложнее (кроме счетчика, сервер посылает затравочное значение, используемое функцией f), но для нас сейчас это не важно. Поскольку функция f необратима, перехват пароля, равно как и получение доступа к серверу аутентификации, не позволяют узнать секретный ключ K и предсказать следующий одноразовый пароль.

Система S/KEY имеет статус Internet-стандарта (RFC 1938).

Другой подход к надежной аутентификации состоит в генерации нового пароля через небольшой промежуток времени (например, каждые 60 секунд), для чего могут использоваться программы или специальные интеллектуальные карты (с практической точки зрения такие пароли можно считать одноразовыми). Серверу аутентификации должен быть известен алгоритм генерации паролей и ассоциированные с ним параметры; кроме того, часы клиента и сервера должны быть синхронизированы.

Сервер аутентификации Kerberos

Kerberos - это программный продукт, разработанный в середине 1980-х годов в Массачусетском технологическом институте и претерпевший с тех пор ряд принципиальных изменений. Клиентские компоненты Kerberos присутствуют в большинстве современных операционных систем.

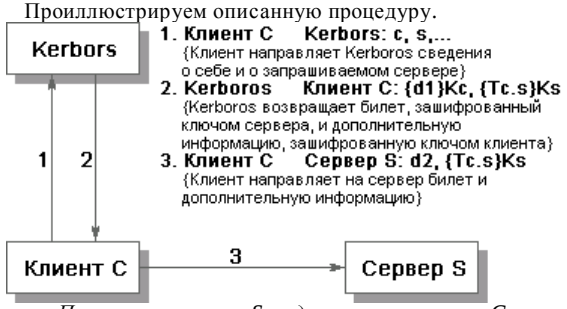
Kerberos предназначен для решения следующей задачи. Имеется открытая (незащищенная) сеть, в узлах которой сосредоточены **субъекты** - пользователи, а также клиентские и серверные программные системы. Каждый субъект обладает секретным ключом. Чтобы субъект C мог доказать свою подлинность субъекту S (без этого S не станет обслуживать C), он должен не только назвать себя, но и продемонстрировать знание секретного ключа. C не может просто послать S свой секретный ключ, во-первых, потому, что сеть открыта (доступна для пассивного и активного прослушивания), а, во-вторых, потому, что S не знает (и не должен знать) секретный ключ C. Требуется менее прямолинейный способ демонстрации знания секретного ключа.

Система Kerberos представляет собой **доверенную третью сторону** (то есть сторону, которой доверяют все), владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности.

Чтобы с помощью Kerberos получить доступ к S (обычно это сервер), C (как правило - клиент) посылает Kerberos запрос, содержащий сведения о нем (клиенте) и о запрашиваемой услуге. В ответ Kerberos возвращает так называемый **билет**, зашифрованный секретным ключом сервера, и копию части информации из билета, зашифрованную секретным ключом клиента. Клиент должен расшифровать вторую порцию данных и переслать ее вместе с билетом серверу. Сервер, расшифровав билет, может сравнить его содержимое с дополнительной информацией, присланной клиентом. Сов-

падение свидетельствует о том, что клиент смог расшифровать предназначенные ему данные (ведь содержимое билета никому, кроме сервера и Kerberos, недоступно), то есть продемонстрировал знание секретного ключа. Значит, клиент - именно тот, за кого себя выдает. Подчеркнем, что секретные ключи в процессе проверки подлинности не передавались по сети (даже в зашифрованном виде) - они только использовались для шифрования. Как организован первоначальный обмен ключами между Kerberos и субъектами и как субъекты хранят свои секретные ключи - вопрос отдельный.

Проиллюстрируем описанную процедуру.



Проверка сервером S подлинности клиента С.

Здесь c и s - сведения (например, имя), соответственно, о клиенте и сервере, d1 и d2 - дополнительная (по отношению к билету) информация, Tc.s - билет для клиента С на обслуживание у сервера S, Kc и Ks - секретные ключи клиента и сервера, {info}K - информация info, зашифрованная ключом K.

Приведенная схема - крайне упрощенная версия реальной процедуры проверки подлинности. Более подробное рассмотрение системы Kerberos можно найти, например, в статье В. Галатенко "Сервер аутентификации Kerberos (Jet Info, 1996, 12-13). Нам же важно отметить, что Kerberos не только устойчив к сетевым угрозам, но и поддерживает концепцию единого входа в сеть.

Идентификация/аутентификация с помощью биометрических данных

Биометрия представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности **отпечатков пальцев**, **сетчатки** и **роговицы глаз, геометрия руки** и **лица** и т.п. К поведенческим характеристикам относятся **динамика подписи** (ручной), стиль **работы с клавиатурой**. На стыке физиологии и поведения находятся анализ особенностей **голоса** и **распознавание речи**.

Биометрией во всем мире занимаются очень давно, однако долгое время все, что было связано с ней, отличалось сложностью и дороговизной. В последнее время спрос на биометрические продукты, в первую очередь в связи с развитием электронной коммерции, постоянно и весьма интенсивно растет. Это понятно, поскольку с точки зрения пользователя гораздо удобнее предъявить себя самого, чем что-то запоминать. Спрос рождает предложение, и на рынке появились относительно недорогие аппаратно-программные продукты, ориентированные в основном на распознавание отпечатков пальцев.

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый **биометрическим шаблоном**) заносится в базу данных (исходные данные, такие как результат сканирования пальца или роговицы, обычно не хранятся).

В дальнейшем для идентификации (и одновременно аутентификации) пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. В случае успешного поиска личность пользователя и ее подлинность считаются установленными. Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных.

Обычно биометрию применяют вместе с другими аутентификаторами, такими, например, как интеллектуальные карты. Иногда биометрическая аутентификация является лишь первым рубежом защиты и служит для активизации интеллектуальных карт, хранящих криптографические секреты; в таком случае биометрический шаблон хранится на той же карте.

Активность в области биометрии очень велика. Организован соответствующий консорциум (см. http://www.biometrics.org), активно ведутся работы по стандартизации разных аспектов технологии (формата обмена данными, прикладного программного интерфейса и т.п.), публикуется масса рекламных статей, в которых биометрия преподносится как средство обеспечения сверхбезопасности, ставшее доступным широким массам.

На наш взгляд, к биометрии следует относиться весьма осторожно. Необходимо учитывать, что она подвержена тем же угрозам, что и другие методы аутентификации. Во-первых, биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения. А, как известно, за время пути... много чего может произойти. Во-вторых, биометрические методы не более надежны, чем база данных шаблонов. В-третьих, следует учитывать разницу между применением биометрии на контролируемой территории, под бдительным оком охраны, и в "полевых" условиях, когда, например к устройству сканирования роговицы могут поднести муляж и т.п. В-четвертых, биометрические данные человека меняются, так что база шаблонов нуждается в сопровождении, что создает определенные проблемы и для пользователей, и для администраторов.

Но главная опасность состоит в том, что любая "пробоина" для биометрии оказывается фатальной. Пароли, при всей их ненадежности, в крайнем случае можно сменить. Утерянную аутентификационную карту можно аннулировать и завести новую. Палец же, глаз или голос сменить нельзя. Если биометрические данные окажутся скомпрометированы, придется как минимум производить существенную модернизацию всей системы.

Управление доступом

Основные понятия

С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над **объектами** (информацией и другими компьютерными ресурсами). В данном разделе речь идет о логическом управлении доступом, которое, в отличие от физического, реализуется программными средствами. Логическое управление доступом - это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

Рассмотрим формальную постановку задачи в традиционной трактовке. Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары "субъект-объект" определить множество допустимых операций (зависящее, быть может, от некоторых дополнительных условий) и контролировать выполнение установленного порядка.

Отношение "субъекты-объекты" можно представить в виде **матрицы доступа**, в строках которой перечислены субъекты, в столбцах - объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа. Фрагмент матрицы может выглядеть, например, так:

Фрагмент матрицы доступа

	Файл	Программа	Линия_связи	Реляционная_таблица
Пользователь_1	orw с системной консоли	e	rw с 8:00 до 18:00	
Пользователь_2				a

"o" - обозначает разрешение на передачу прав доступа другим пользователям,
"r" - чтение,
"w" - запись,
"e" - выполнение,
"a" - добавление информации

Тема логического управления доступом - одна из сложнейших в области информационной безопасности. Дело в том, что само понятие объекта (а тем более видов доступа) меняется от сервиса к сервису. Для операционной системы к объектам относятся файлы, устройства и процессы. Применительно к файлам и устройствам обычно рассматриваются права на чтение, запись, выполнение (для программных файлов), иногда на удаление и добавление. Отдельным правом может быть возможность передачи полномочий доступа другим субъектам (так называемое право владения). Процессы можно создавать и уничтожать. Современные операционные системы могут поддерживать и другие объекты.

Для систем управления реляционными базами данных объект - это база данных, таблица, представление, хранимая процедура. К таблицам применимы операции поиска, добавления, модификации и удаления данных, у других объектов иные виды доступа.

Разнообразие объектов и применимых к ним операций приводит к принципиальной децентрализации логического управления доступом. Каждый сервис должен сам решать, позволить ли конкретному субъекту ту или иную операцию. Теоретически это согласуется с современным объектно-ориентированным подходом, на практике же приводит к значительным трудностям. Главная проблема в том, что ко многим объектам можно получить доступ с помощью разных сервисов (возможно, при этом придется преодолеть некоторые технические трудности). Так, до реляционных таблиц можно добраться не только средствами СУБД, но и путем непосредственного чтения файлов или дисковых разделов, поддерживаемых операционной системой (разобравшись предварительно в структуре хранения объектов базы данных). В результате при задании матрицы доступа нужно принимать во внимание не только принцип распределения привилегий для каждого сервиса, но и существующие связи между сервисами (приходится заботиться о согласованности разных частей матрицы). Аналогичная трудность возникает при экспорте/импорте данных, когда информация о правах доступа, как правило, теряется (поскольку на новом сервисе она не имеет смысла). Следовательно, обмен данными между различными сервисами представляет особую опасность с точки зрения управления доступом, а при проектировании и реализации разнородной конфигурации необходимо

позаботиться о согласованном распределении прав доступа субъектов к объектам и о минимизации числа способов экспорта/импорта данных.

При принятии решения о предоставлении доступа обычно анализируется следующая информация:

- идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера и т.п.). Подобные идентификаторы являются основой произвольного (или дискреционного) управления доступом;
- атрибуты субъекта (метка безопасности, группа пользователя и т.п.). Метки безопасности - основа принудительного (мандатного) управления доступом.

Матрицу доступа, ввиду ее разреженности (большинство клеток - пустые), неразумно хранить в виде двухмерного массива. Обычно ее хранят по столбцам, то есть для каждого объекта поддерживается список "допущенных" субъектов вместе с их правами. Элементами списков могут быть имена групп и шаблоны субъектов, что служит большим подспорьем администратору. Некоторые проблемы возникают только при удалении субъекта, когда приходится удалять его имя из всех списков доступа; впрочем, эта операция производится нечасто.

Списки доступа - исключительно гибкое средство. С их помощью легко выполнить требование о гранулярности прав с точностью до пользователя. Посредством списков несложно добавить права или явным образом запретить доступ (например, чтобы наказать нескольких членов группы пользователей). Безусловно, списки являются лучшим средством произвольного управления доступом.

Подавляющее большинство операционных систем и систем управления базами данных реализуют именно произвольное управление доступом. Основное достоинство произвольного управления - гибкость. Вообще говоря, для каждой пары "субъект-объект" можно независимо задавать права доступа (особенно легко это делать, если используются **списки управления доступом**). К сожалению, у "произвольного" подхода есть ряд недостатков. Рассредоточенность управления доступом ведет к тому, что доверенными должны быть многие пользователи, а не только системные операторы или администраторы. Из-за рассеянности или некомпетентности сотрудника, владеющего секретной информацией, эту информацию могут узнать и все остальные пользователи. Следовательно, произвольность управления должна быть дополнена жестким контролем за реализацией избранной политики безопасности.

Второй недостаток, который представляется основным, состоит в том, что права доступа существуют отдельно от данных. Ничто не мешает пользователю, имеющему доступ к секретной информации, записать ее в доступный всем файл или заменить полезную утилиту ее "троянским" аналогом. Подобная "разделенность" прав и данных существенно осложняет проведение несколькими системами согласованной политики безопасности и, главное, делает практически невозможным эффективный контроль согласованности.

Возвращаясь к вопросу представления матрицы доступа, укажем, что для этого можно использовать также функциональный способ, когда матрицу не хранят в явном виде, а каждый раз вычисляют содержимое соответствующих клеток. Например, при принудительном управлении доступом применяется сравнение меток безопасности субъекта и объекта.

Удобной надстройкой над средствами логического управления доступом является **ограничивающий интерфейс**, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ. Подобный подход обычно реализуют в рамках системы меню (пользователю показывают лишь допустимые варианты выбора) или посредством ограничивающих оболочек, таких как restricted shell в ОС Unix.

В заключение подчеркнем важность управления доступом не только на уровне операционной системы, но и в рамках других сервисов, входящих в состав современных приложений, а также, насколько это возможно, на "стыках" между сервисами. Здесь на первый план выходит существование единой политики безопасности организации, а также квалифицированное и согласованное системное администрирование.

Ролевое управление доступом

При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов. Необходимы решения в объектно-ориентированном стиле, способные эту сложность понизить.

Таким решением является **ролевое управление доступом** (РУД). Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности - роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права.

Пользователи, объекты и роли.

Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах. Кроме того, ролей должно быть значительно меньше, чем пользователей. В результате число администрируемых связей становится пропорциональным сумме (а не произведению) количества пользователей и объектов, что по порядку величины уменьшить уже невозможно.

Ролевой доступ развивается более 10 лет (сама идея ролей, разумеется, значительно старше) как на уровне операционных систем, так и в рамках СУБД и других информационных сервисов. В частности, существуют реализации ролевого доступа для Web-серверов.

В 2001 году Национальный институт стандартов и технологий США предложил проект стандарта ролевого управления доступом (см. http://csrc.nist.gov/rbac/), основные положения которого мы и рассмотрим.

Ролевое управление доступом оперирует следующими основными понятиями:

- пользователь (человек, интеллектуальный автономный агент и т.п.);
- сеанс работы пользователя;
- роль (обычно определяется в соответствии с организационной структурой);
- объект (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД);
- операция (зависит от объекта; для файлов ОС - чтение, запись, выполнение и т.п.; для таблиц СУБД - вставка, удаление и т.п., для прикладных объектов операции могут быть более сложными);
- право доступа (разрешение выполнять определенные операции над определенными объектами).

Ролям приписываются пользователи и права доступа; можно считать, что они (роли) именуют отношения "многие ко многим" между пользователями и правами. Роли могут быть приписаны многие пользователи; один пользователь может быть приписан нескольким ролям. Во время сеанса работы пользователя активизируется подмножество ролей, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным ролям. Одновременно пользователь может открыть несколько сеансов.

Между ролями может быть определено отношение частичного порядка, называемое наследованием. Если роль r2 является наследницей r1, то все права r1 приписываются r2, а все пользователи r2 приписываются r1. Очевидно, что **наследование ролей** соответствует наследованию классов в объектно-ориентированном программировании, только правам доступа соответствуют методы классов, а пользователям - объекты (экземпляры) классов.

Отношение наследования является иерархическим, причем права доступа и пользователи распространяются по уровням иерархии навстречу друг другу. В общем случае наследование является множественным, то есть у одной роли может быть несколько предшественниц (и, естественно, несколько наследниц, которых мы будем называть также преемницами).

Можно представить себе формирование **иерархии ролей**, начиная с минимума прав (и максимума пользователей), приписываемых роли "сотрудник", с постепенным уточнением состава пользователей и добавлением прав (роли "системный администратор", "бухгалтер" и т.п.), вплоть до роли "руководитель" (что, впрочем, не значит, что руководителю предоставляются неограниченные права; как и другим ролям, в соответствии с принципом **минимизации привилегий**, этой роли целесообразно разрешить только то, что необходимо для выполнения служебных обязанностей). Фрагмент подобной иерархии ролей показан на рис.

Фрагмент иерархии ролей.

Для реализации еще одного упоминавшегося ранее важного принципа информационной безопасности вводится понятие **разделения обязанностей**, причем в двух видах: статическом и динамическом.

Статическое разделение обязанностей налагает ограничения на **приписывание пользователей ролям**. В простейшем случае членство в некоторой роли запрещает приписывание пользователя определенному множеству других ролей. В общем случае данное ограничение задается как пара "множество ролей - число" (где множество состоит, по крайней мере, из двух ролей, а число должно быть больше 1), так что никакой пользователь не может быть приписан

указанному (или большему) числу ролей из заданного множества. Например, может существовать пять бухгалтерских ролей, но политика безопасности допускает членство не более чем в двух таких ролях (здесь число=3).

При наличии наследования ролей ограничение приобретает несколько более сложный вид, но суть остается простой: при проверке членства в ролях нужно учитывать приписывание пользователей ролям-наследницам.

Динамическое разделение обязанностей отличается от статического только тем, что рассматриваются роли, одновременно активные (быть может, в разных сеансах) для данного пользователя (а не те, которым пользователь статически приписан). Например, один пользователь может играть роль и кассира, и контролера, но не одновременно; чтобы стать контролером, он должен сначала закрыть кассу. Тем самым реализуется так называемое **временное ограничение доверия**, являющееся аспектом минимизации привилегий.

Рассматриваемый проект стандарта содержит спецификации трех категорий функций, необходимых для администрирования РУД:

1. Административные функции (создание и сопровождение ролей и других атрибутов ролевого доступа): создать/удалить роль/пользователя, приписать пользователя/право роли или ликвидировать существующую ассоциацию, создать/удалить отношение наследования между существующими ролями, создать новую роль и сделать ее наследницей/предшественницей существующей роли, создать/удалить ограничения для статического/динамического разделения обязанностей.
2. Вспомогательные функции (обслуживание сеансов работы пользователей): открыть сеанс работы пользователя с активацией подразумеваемого набора ролей; активировать новую роль, деактивировать роль; проверить правомерность доступа.
3. Информационные функции (получение сведений о текущей конфигурации с учетом отношения наследования). Здесь проводится разделение на обязательные и необязательные функции. К числу первых принадлежат получение списка пользователей, приписанных роли, и списка ролей, которым приписан пользователь.

Все остальные функции отнесены к разряду необязательных. Это получение информации о правах, приписанных роли, о правах заданного пользователя (которыми он обладает как член множества ролей), об активных в данный момент сеанса ролях и правах, об операциях, которые роль/пользователь правомочны совершить над заданным объектом, о статическом/динамическом разделении обязанностей.

Можно надеяться, что предлагаемый стандарт поможет сформировать единую терминологию и, что более важно, позволит оценивать РУД-продукты с единых позиций, по единой шкале.

Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. С одной стороны, это создает новую проблему распространения ключей. С другой стороны, получатель на основании наличия зашифрованного и расшифрованного сообщения не может доказать, что он получил это сообщение от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать самостоятельно.

В асимметричных методах используются два ключа. Один из них, несекретный (он может публиковаться вместе с другими открытыми сведениями о пользователе), применяется для шифрования, другой (секретный, известный только получателю) - для расшифрования. Самым популярным из асимметричных является метод RSA (Райвест, Шамир, Адлеман), основанный на операциях с большими (скажем, 100-значными) простыми числами и их произведениями.

Проиллюстрируем использование асимметричного шифрования (см. рис.).

Использование асимметричного метода шифрования.

Существенным недостатком асимметричных методов шифрования является их низкое быстродействие, поэтому данные методы приходится сочетать с симметричными (асимметричные методы на 3 - 4 порядка медленнее). Так, для решения задачи эффективного шифрования с передачей секретного ключа, использованного отправителем, сообщение сначала симметрично зашифровывают случайным ключом, затем этот ключ зашифровывают открытым асимметричным ключом получателя, после чего сообщение и ключ отправляются по сети.

Отметим, что асимметричные методы позволили решить важную задачу совместной выработки секретных ключей (это существенно, если стороны не доверяют друг другу), обслуживающих сеанс взаимодействия, при изначальном отсутствии общих секретов. Для этого используется алгоритм Диффи-Хелмана.

Определенное распространение получила разновидность симметричного шифрования, основанная на использовании составных ключей. Идея состоит в том, что секретный ключ делится на две части, хранящиеся отдельно. Каждая часть сама по себе не позволяет выполнить расшифрование. Если у правоохранительных органов появляются подозрения относительно лица, использующего некоторый ключ, они могут в установленном порядке получить половинки ключа и дальше действовать обычным для симметричного расшифрования образом.

Порядок работы с составными ключами - хороший пример следования принципу разделения обязанностей. Он позволяет сочетать права на разного рода тайны (персональную, коммерческую) с возможностью эффективно следить за нарушителями закона, хотя, конечно, здесь очень много тонкостей и технического, и юридического плана.

Расшифрование эффективно зашифрованного сообщения.

Многие криптографические алгоритмы в качестве одного из параметров требуют псевдослучайное значение, в случае предсказуемости которого в алгоритме появляется уязвимость (подобное уязвимое место было обнаружено в некоторых вариантах Web-навигаторов). Генерация псевдослучайных последовательностей - важный аспект криптографии, на котором мы, однако, останавливаться не будем.

Более подробную информацию о компьютерной криптографии можно почерпнуть из статьи Г. Семенова "Не только шифрование, или Обзор криптотехнологий" (Jet Info, 2001, 3).

Контроль целостности

Криптографические методы позволяют надежно контролировать целостность как отдельных порций данных, так и их наборов (таких как поток сообщений); определять подлинность источника данных; гарантировать невозможность отказаться от совершенных действий ("неотказуемость").

В основе криптографического контроля целостности лежат два понятия:

- хэш-функция;
- электронная цифровая подпись (ЭЦП).

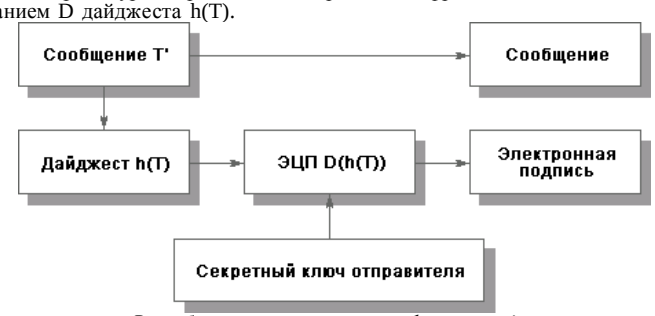
Хэш-функция - это труднообратимое преобразование данных (односторонняя функция), реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хэш-функции.

Пусть имеются данные, целостность которых нужно проверить, хэш-функция и ранее вычисленный результат ее применения к исходным данным (так называемый дайджест). Обозначим хэш-функцию через h, исходные данные - через T, проверяемые данные - через T'. Контроль целостности данных сводится к проверке равенства h(T') = h(T). Если оно выполнено, считается, что T' = T. Совпадение дайджестов для различных данных называется коллизией. В принципе, коллизии, конечно, возможны, поскольку мощность множества дайджестов меньше, чем мощность множества хэшируемых данных, однако то, что h есть функция односторонняя, означает, что за приемлемое время специально организовать коллизию невозможно.

Рассмотрим теперь применение асимметричного шифрования для выработки и проверки электронной цифровой подписи. Пусть E(T) обозначает результат зашифрования текста T с помощью открытого ключа, а D(T) - результат расшифрования текста T (как правило, шифрованного) с помощью секретного ключа. Чтобы асимметричный метод мог применяться для реализации ЭЦП, необходимо выполнение тождества

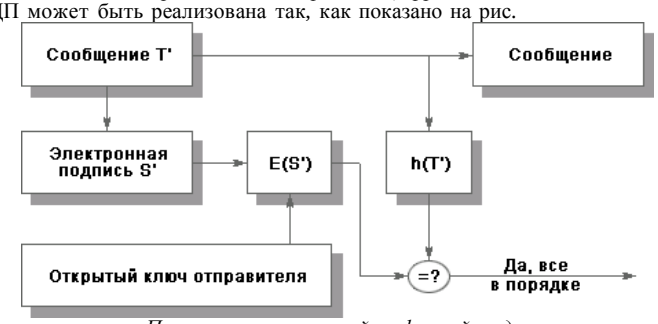
E(D(T)) = D(E(T)) = T

На рис. показана процедура выработки электронной цифровой подписи, состоящая в шифровании преобразованием D дайджеста h(T).



Выработка электронной цифровой подписи.

Проверка ЭЦП может быть реализована так, как показано на рис.



Проверка электронной цифровой подписи.

Из равенства

E(S') = h(T')

следует, что S' = D(h(T')) (для доказательства достаточно применить к обеим частям преобразование D и вычеркнуть в левой части тождественное преобразование D(E())). Таким образом, электронная цифровая подпись защищает целостность сообщения и удостоверяет личность отправителя, то есть защищает целостность источника данных и служит основой неотказуемости.

Два российских стандарта, ГОСТ Р 34.10-94 "Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма" и ГОСТ Р 34.11-94 "Функция хэширования", объединенные общим заголовком "Информационная технология. Криптографическая защита информации", регламентируют вычисление дайджеста и реализацию ЭЦП. В сентябре 2001 года был утвержден, а 1 июля 2002 года вступил в силу новый стандарт ЭЦП - ГОСТ Р 34.10-2001, разработанный специалистами ФАПСИ.

Для контроля целостности последовательности сообщений (то есть для защиты от кражи, дублирования и переупорядочения сообщений) применяют временные штампы и нумерацию элементов последовательности, при этом штампы и номера включают в подписываемый текст.

Цифровые сертификаты

При использовании асимметричных методов шифрования (и, в частности, электронной цифровой подписи) необходимо иметь гарантию подлинности пары (имя пользователя, открытый ключ пользователя). Для решения этой задачи в спецификациях X.509 вводятся понятия цифрового сертификата и удостоверяющего центра.

Удостоверяющий центр - это компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей. Открытые ключи и другая информация о пользователях хранится удостоверяющими центрами в виде цифровых сертификатов, имеющих следующую структуру:

- порядковый номер сертификата;
- идентификатор алгоритма электронной подписи;
- имя удостоверяющего центра;
- срок годности;
- имя владельца сертификата (имя пользователя, которому принадлежит сертификат);
- открытые ключи владельца сертификата (ключей может быть несколько);

- идентификаторы алгоритмов, ассоциированных с открытыми ключами владельца сертификата;
- электронная подпись, сгенерированная с использованием секретного ключа удостоверяющего центра (подписывается результат хэширования всей информации, хранящейся в сертификате).

Цифровые сертификаты обладают следующими свойствами:

- любой пользователь, знающий открытый ключ удостоверяющего центра, может узнать открытые ключи других клиентов центра и проверить целостность сертификата;
- никто, кроме удостоверяющего центра, не может модифицировать информацию о пользователе без нарушения целостности сертификата.

В спецификациях X.509 не описывается конкретная процедура генерации криптографических ключей и управления ими, однако даются некоторые общие рекомендации. В частности, оговаривается, что пары ключей могут порождаться любым из следующих способов.

- ключи может генерировать сам пользователь. В таком случае секретный ключ не попадает в руки третьих лиц, однако нужно решать задачу безопасной связи с удостоверяющим центром;
- ключи генерирует доверенное лицо. В таком случае приходится решать задачи безопасной доставки секретного ключа владельцу и предоставления доверенных данных для создания сертификата;
- ключи генерируются удостоверяющим центром. В таком случае остается только задача безопасной передачи ключей владельцу.

Цифровые сертификаты в формате X.509 версии 3 стали не только формальным, но и фактическим стандартом, поддерживаемым многочисленными удостоверяющими центрами.

Комплексная система безопасности

Классификация информационных объектов

Обрабатываемые данные могут классифицироваться согласно различным категориям информационной безопасности: требованиям к их доступности (безотказности служб), целостности, конфиденциальности.

Классификация по требуемой степени безотказности

От различных типов данных требуется различная степень безотказности доступа. Тратить большие деньги на системы безотказности для не очень важной информации невыгодно и даже убыточно, но нельзя и неправильно оценивать действительно постоянно требуемую информацию – ее отсутствие в неподходящий момент также может принести значительные убытки.

Безотказность, или надежность доступа к информации, является одной из категорий информационной безопасности. Предлагается следующая схема классификации информации на 4 уровня безотказности.

Параметр	класс 0	класс 1	класс 2	класс 3
Максимально возможное непрерывное время отказа	1 неделя	1 сутки	1 час	1 час
В какое время время отказа не может превышать указанное выше ?	в рабочее	в рабочее	в рабочее	24 часа в сутки
Средняя вероятность доступности данных в произвольный момент времени	80%	95%	99.5%	99.9%
Среднее максимальное время отказа	1 день в неделю	2 часа в неделю	20 минут в неделю	12 минут в месяц

Классификация по уровню конфиденциальности

Классификация по степени конфиденциальности – одна из основных и наиболее старых классификаций данных. Она применялась еще задолго до появления вычислительной техники и с тех пор изменилась незначительно.

Уровень конфиденциальности информации является одной из самых важных категорий, принимаемых в рассмотрение при создании определенной политики безопасности учреждения. Предлагается следующая схема классификации информации на 4 класса по уровню ее конфиденциальности.

Класс	Тип информации	Описание	Примеры
0	открытая информация	общедоступная информация	информационные брошюры, сведения публикававшиеся в СМИ
1	внутренняя информация	информация, недоступная в открытом виде, но не несущая никакой опасности при ее раскрытии	финансовые отчеты и тестовая информация за давно прошедшие периоды, отчеты об обычных заседаниях и встречах, внутренний телефонный справочник

			фирмы
2	конфиденциальная информация	раскрытие информации ведет к значительным потерям на рынке	реальные финансовые данные, планы, проекты, полный набор сведений о клиентах, информация о бывших и нынешних проектах с нарушениями этических норм
3	секретная информация	раскрытие информации приведет к финансовой гибели компании	(зависит от ситуации)

Требования по работе с конфиденциальной информацией

Различные классы конфиденциальной информации необходимо снабжать различными по уровню безопасности системами технических и административных мер.

При работе с информацией 1-го класса конфиденциальности рекомендуется выполнение следующих требований:

- осведомление сотрудников о закрытости данной информации,
- общее ознакомление сотрудников с основными возможными методами атак на информацию
- ограничение физического доступа
- полный набор документации по правилам выполнения операций с данной информацией

При работе с информацией 2-го класса конфиденциальности к перечисленным выше требованиям добавляются следующие:

- расчет рисков атак на информацию
- поддержания списка лиц, имеющих доступ к данной информации
- по возможности выдача подобной информации по расписку (в т.ч. электронную)
- автоматическая система проверки цлостности системы и ее средств безопасности
- надежные схемы физической ранспортировки
- обязательное шифрование при передаче по линиям связи
- схема бесперебойного питания ЭВМ

При работе с информацией 3-го класса конфиденциальности ко всем перечисленным выше требованиям добавляются следующие:

- детальный план спасения либо надежного уничтожения информации в аварийных ситуациях (пожар, наводнение, взрыв)
- защита ЭВМ либо носителей информации от повреждения водой и высокой температурой
- криптографическая проверка целостности информации

Политика ролей

Ролями называются характерные наборы функций и степени ответственности, свойственные теми или иными группами лиц. Четкое определение ролей, классификация их уровней доступа и ответственности, составление списка соответствия персонала тем или иным ролям делает политику безопасности в отношении рабочих и служащих предприятия четкой, ясной и легкой для исполнения и проверки.

Функции каждого человека, так или иначе связанного с конфиденциальной информацией на предприятии, можно классифицировать и в некотором приближении формализовать. Подобное общее описание функций оператора носит название роли. В зависимости от размеров предприятия некоторые из перечисленных ниже ролей могут отсутствовать вообще, а некоторые могут совмещаться одним и тем же физическим лицом.

Специалист по информационной безопасности играет основную роль в разработке и поддержании политики безопасности предприятия. Он проводит расчет и перерасчет рисков, ответственен за поиск самой свежей информации об обнаруженных уязвимостях в используемом в фирме программном обеспечении и в целом в стандартных алгоритмах.

Владелец информации – лицо, непосредственно работающее с данной информацией, (не нужно путать с оператором). Зачастую только он в состоянии реально оценить класс обрабатываемой информации, а иногда и рассказать о нестандартных методах атак на нее (узкоспецифичных для этого вида данных). Владелец информации не должен участвовать в аудите системы безопасности.

Поставщик аппаратного и программного обеспечения. Обычно стороннее лицо, которое несет ответственность перед фирмой за поддержание должного уровня информационной безопасности в поставляемых им продуктов.

Разработчик системы и/или программного обеспечения играет основную роль в уровне безопасности разрабатываемой системы. На этапах планирования и разработки должен активно взаимодействовать со специалистами по информационной безопасности.

Линейный менеджер или менеджер отдела является промежуточным звеном между операторами и специалистами по информационной безопасности. Его задача – своевременно и качественно инструктировать подчиненный ему персонал обо всех требованиях службы безопасности и следить за ее их выполнением на рабочих местах. Линейные менеджеры должны быть осведомлены о всей

политике безопасности предприятия, но доводить до сведения подчиненных только те ее аспекты, которые непосредственно их касаются.

Операторы – лица, ответственные только за свои поступки. Они не принимают никаких решений и ни за кем не наблюдают. Они должны быть осведомлены о классе конфиденциальности информации, с которой они работают, и о том, какой ущерб будет нанесен фирмы при ее раскрытии.

Аудиторы – внешние специалисты или фирмы, нанимаемые предприятием для периодической (довольно редкой) проверки организации и функционирования всей системы безопасности.

Создание политики информационной безопасности

Методика создания политики безопасности предприятия состоит из учета основных (наиболее опасных) рисков информационных атак, современной ситуации, факторов непреодолимой силы и генеральной стоимости проекта.

Политика безопасности – это комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии. Политика безопасности включает в себя требования в адрес персонала, менеджеров и технических служб. Основные направления разработки политики безопасности:

- определение какие данные и насколько серьезно необходимо защищать,
- определение кто и какой ущерб может нанести фирме в информационном аспекте,
- вычисление рисков и определение схемы уменьшения их до приемлемой величины.

Существуют две системы оценки текущей ситуации в области информационной безопасности на предприятии. Они получили образные названия "исследование снизу вверх" и "исследование сверху вниз". Первый метод достаточно прост, требует намного меньших капитальных вложений, но и обладает меньшими возможностями. Он основан на известной схеме: "Вы – злоумышленник. Ваши действия ?". То есть служба информационной безопасности, основываясь на данных о всех известных видах атак, пытается применить их на практике с целью проверки, а возможно ли такая атака со стороны реального злоумышленника.

Метод "сверху вниз" представляет собой, наоборот, детальный анализ всей существующей схемы хранения и обработки информации. Первым этапом этого метода является, как и всегда, определение, какие информационные объекты и потоки необходимо защищать. Далее следует изучение текущего состояния системы информационной безопасности с целью определения, что из классических методик защиты информации уже реализовано, в каком объеме и на каком уровне. На третьем этап производится классификация всех информационных объектов на классы в соответствии с ее конфиденциальностью, требованиями к доступности и целостности (неизменности).

Далее следует выяснение насколько серьезный ущерб может принести фирме раскрытие или иная атака на каждый конкретный информационный объект. Этот этап носит название "вычисление рисков". В первом приближении риском называется произведение "возможного ущерба от атаки" на "вероятность такой атаки". Существует множество схем вычисления рисков, остановимся на одной из самых простых.

Ущерб от атаки может быть представлен неотрицательным числом в приблизительном соответствии со следующей таблицей:

Величина ущерба	Описание
0	Раскрытие информации принесет ничтожный моральный и финансовый ущерб фирме
1	Ущерб от атаки есть, но он незначителен, основные финансовые операции и положение фирмы на рынке не затронуты
2	Финансовые операции не ведутся в течение некоторого времени, за это время фирма терпит убытки, но ее положение на рынке и количество клиентов изменяются минимально
3	Значительные потери на рынке и в прибыли. От фирмы уходит ощутимая часть клиентов
4	Потери очень значительны, фирма на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы.
5	Фирма прекращает существование

Вероятность атаки представляется неотрицательным числом в приблизительном соответствии со следующей таблицей:

Вероятность	Средняя частота появления
0	Данный вид атаки отсутствует
1	реже, чем раз в год
2	около 1 раза в год
3	около 1 раза в месяц
4	около 1 раза в неделю
5	практически ежедневно

Необходимо отметить, что классификацию ущерба, наносимого атакой, должен оценивать владелец информации, или работающий с нею персонал. А вот оценку вероятности появления атаки лучше доверять техническим сотрудникам фирмы.

Следующим этапом составляется таблица рисков предприятия. Она имеет следующий вид:

Описание атаки	Ущерб	Вероятность	Риск (=Ущерб*Вероятность)
Спам (переполнение почтового ящика)	1	4	4
Копирование жесткого диска из центрального офиса	3	1	3
...	...	...	2
		Итого:	9

На этапе анализа таблицы рисков задаются некоторым максимально допустимым риском, например значением 7. Сначала проверяется каждая строка таблицы на не превышение риска этого значения. Если такое превышение имеет место, значит, данная строка – это одна из первоочередных целей разработки политики безопасности. Затем производится сравнение удвоенного значения (в нашем случае 7*2=14) с интегральным риском (ячейка "Итого"). Если интегральный риск превышает допустимое значение, значит, в системе набирается множество мелких погрешностей в системе безопасности, которые в сумме не дадут предприятию эффективно работать. В этом случае из строк выбираются те, которые дает самый значительный вклад в значение интегрального риска и производится попытка их уменьшить или устранить полностью.

На самом ответственном этапе производится собственно разработка политики безопасности предприятия, которая обеспечит надлежащие уровни как отдельных рисков, так и интегрального риска. При ее разработке необходимо, однако, учитывать объективные проблемы, которые могут встать на пути реализации политики безопасности. Такими проблемами могут стать законы страны и международного сообщества, внутренние требования корпорации, этические нормы общества.

После описания всех технических и административных мер, планируемых к реализации, производится расчет экономической стоимости данной программы. В том случае, когда финансовые вложения в программу безопасности являются неприемлемыми или просто экономически невыгодными по сравнению с потенциальным ущербом от атак, производится возврат на уровень, где мы задавались максимально допустимым риском 7 и увеличение его на один или два пункта.

Завершается разработка политики безопасности ее утверждением у руководства фирмы и детальным документированием. За этим должна следовать активная реализация всех указанных в плане компонентов. Перерасчет таблицы рисков и, как следствие, модификация политики безопасности фирмы чаще всего производится раз в два года.

Методы обеспечения безотказности

Безотказность сервисов и служб хранения данных достигается с помощью систем самотестирования и внесения избыточности на различных уровнях: **аппаратном, программном, информационном.**

Методы поддержания безотказности являются смежной областью в схемах комплексной информационной безопасности предприятия. Основным методом в этой сфере является внесение избыточности. Она может реализовываться в системе на трех уровнях: уровне данных (или информации), уровне сервисов (или приложений) и уровне аппаратного обеспечения.

Внесение избыточности на уровне данных практикуется достаточно давно: это резервное копирование и помехоустойчивое кодирование. Резервное копирование выполняется обычно при хранении информации на современных запоминающих устройствах (поскольку для них в аварийной ситуации характерен выход из строя больших блоков данных целиком – трудно восстановимое с помощью помехоустойчивого кодирование повреждение). А вот использование кодов с обнаружением и некоторым потенциалом для исправления ошибок получило широкое применение в средствах телекоммуникации.

Внесение избыточности на уровне приложений используется гораздо реже. Однако, многие, особенно сетевые, службы изначально поддерживают возможность работы с резервным или вообще с неограниченным заранее неизвестным количеством альтернативных служб. Введение такой возможности рекомендуется при разработке программного обеспечения, однако, сам процесс автоматического переключения на альтернативную службу должен подтверждаться криптографическим обменом первоначальной (установочной) информацией. Это необходимо делать для того, чтобы злоумышленник не мог, выведя из строя реальный сервис, навязать Вашей программе свой сервис с фальсифицированной информацией.

Внесение избыточности на аппаратном уровне реализуется обычно в отношении периферийных устройств (накопители на гибких и жестких дисках, сетевые и видео- адаптеры, мониторы, устройства ввода информации от пользователя). Это связано с тем, что дублирование работы основных компонентов ЭВМ (процессора, ОЗУ) гораздо проще выполнить, установив просто полноценную дублирующую ЭВМ с теми же функциями. Для автоматического определения работоспособности

ЭВМ в программное обеспечение встраиваются либо 1) проверка контрольных сумм информации, либо 2) тестовые примеры с заведомо известным результатом, запускаемые время от времени, либо 3) монтирование трех и более дублирующих устройств и сверка их выходных результаты по мажоритарному правилу (каких результатов больше – те и есть правильные, а машины, выдавшие не такие результаты, выведены из строя).

Организация пропускного режим – первый шаг к обеспечению безопасности и конфиденциальности информации

При комплексном обеспечении безопасности конфиденциальной информации важное значение имеет организация пропускного режима в фирме. Основными задачами пропускного режима (как известно) являются:

- обеспечение установленного порядка вноса (выноса), либо ввоза (вывоза) материальных ценностей;
- пресечение несанкционированного проникновения посторонних лиц в выделенные помещения и на объекты вычислительной техники фирмы.

Пропускные документы

Виды пропусков.

Для организации пропускного режима сотрудникам фирмы должны быть выданы пропускные документы.

В качестве пропускных документов могут быть: удостоверения, пропуска. В свою очередь пропуска бывают двух видов: для сотрудников (посетителей) и материальные.

Сотрудникам (посетителям) могут выдаваться пропуска 3-х видов:

- разовые;
- временные;
- постоянные.

Разовые пропуска выдаются, как правило, посетителям. Они действительны в течение 30 минут с момента их выдачи до прохода контрольно-пропускного поста (КПП) и в течение 15 минут после отметки о времени ухода посетителя. Отметка о времени ухода посетителя делается на обратной стороне разового пропуска руководителем подразделения, которое посещал посетитель.

Прикомандированным сотрудникам, либо сотрудникам, работающим временно, выдаются временные пропуска. Временные пропуска могут быть с фотографиями и без них. С фотографиями временные пропуска выдаются - на срок до 3-х месяцев, без фотографий на срок до 1 месяца. Удостоверения и постоянные пропуска выдают на срок до нескольких лет. Через 1-2 года осуществляется их перерегистрация путем проставления соответствующей отметки.

Материальные пропуска выдаются на внос (вынос), либо ввоз (вывоз) материальных ценностей. По срокам действия они приравниваются к разовым пропускам. Для повышения эффективности службы пропускного режима в настоящее время широкое применение находят технические средства, получившие название системы ограничения и контроля доступа (СО и КД).

Грамотное использование СО и КД позволит надежно обеспечить защиту от несанкционированного доступа не только на территорию фирмы, но и в выделенные помещения и на объекты вычислительной техники. То есть на объекты, где обрабатывается конфиденциальная информация. Структурная схема системы ограничения и контроля доступа показана на Рис.

Структурная схема системы ограничения и контроля доступа . Как видно из рисунка основными элементами СО и КД являются:

- считыватель;
- контролер;
- исполнительное устройство.

Для более сложных систем применяются системы централизованного управления. Они состоят из компьютера (может быть система компьютеров, объединенных в локальную сеть) с мощным программным обеспечением.

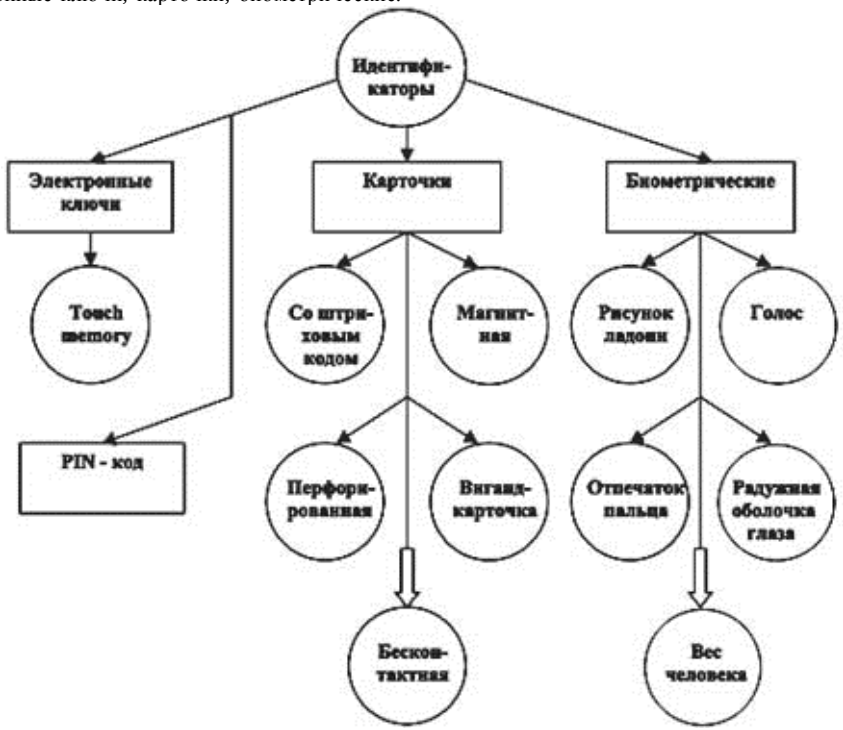
Считыватель - это устройство (размещенное в двери или рядом с дверью), предназначенное для считывания специальной кодовой информации, записанной на идентификаторе и передаче этой информации в виде определенного сигнала в контролер.

Контролер предназначен для приема и анализа информации, переданной считывателем, сравнения этой информации с эталонной, принятие на этой основе решения о допуске посетителя и выдачи сигнала управления на исполнительное устройство и в систему централизованного управления (при ее наличии).

В качестве исполнительных устройств могут быть электромеханические (электромагнитные) замки, а также устройства управления калитками, воротами, турникетами и т.д.

Для того, чтобы посетитель попал на объект (в помещение) он должен предъявить считывателю свой идентификатор. Таким образом, идентификатор - это устройство, в которое записывается кодовая информация, однозначно идентифицирующая его владельца.

Классификация идентификаторов, показана на Рис.4. Идентификаторов бывает несколько видов: электронные ключи, карточки, биометрические.



Классификация идентификаторов.

Электронные ключи "Touch Memory" представляют собой микросхему, расположенную в прочном металлическом корпусе. Кодовая информация записывается в память данной схемы. Код с электронного ключа считывается при его касании считывателя.

Карточка со штриховым кодом представляет собой пластину с нанесенными на нее полосами черного цвета (штрихами). Кодовая информация содержится в изменяющейся ширине штрихов и расстоянии между ними. Код с такой карточки считывается оптическим считывателем. На магнитную карточку кодовая информация записывается на магнитной полосе.

Перфорированная карточка представляет собой пластину (пластмассовую или металлическую). Кодовая информация на перфорированную карточку наносится в виде отверстий, расположенных в определенном порядке. Код с карточек считывается механическими или оптическими считывателями.

Кодовая информация на Виганд-карточке представляет собой определенным образом расположенные тонкие металлические проволочки, приклеенные на карточке специальным клеем. Информация с карточки считывается электромагнитным считывателем.

Бесконтактная карточка (Proximity) кодовую информацию хранит в микросхеме. Кодовая информация с бесконтактных карточек считывается радиочастотным считывателем.

В последнее время находят применение так называемые биометрические идентификаторы. Хотя отношение к ним специалистов носит противоречивый характер. В качестве идентификационных признаков могут быть использованы:

- рисунок ладони;
- голос человека;
- отпечаток пальца;
- радужная оболочка глаза;
- вес человека и т.д.

Особое место среди идентификаторов занимают PIN-коды. Носителем кодовой информации является память человека. Сотрудник самостоятельно набирает на клавиатуре код и таким образом управляет исполнительным устройством (замком двери, например).

Используя на практике СО и КД можно с большой эффективностью обеспечить пропускной режим, как на территорию фирмы, так и в ее отдельные помещения. Надежно решить, таким образом, проблему защиты от несанкционированного доступа злоумышленников в служебные помещения фирмы, а также проблему от несанкционированного выноса (вывоза) материальных ценностей фирмы.

С другой стороны СО и КД позволит также эффективно решать задачи защиты конфиденциальной информации, обрабатываемой в некоторых помещениях фирмы. Это позволит не только повысить безопасность в целом фирмы как объекта, но и безопасность сведений, относящихся к коммерческой тайне фирмы, что в свою очередь снижает общие затраты на обеспечение безопасности фирмы.

Лекция 10. Обзор биометрических технологий

Вот и наступило время, когда сканирование сетчатки глаза, отпечатков пальцев или проверка по голосу из разряда атрибутов шпионских боевиков и фильмов о будущем стали в один ряд с другими решениями по обеспечению безопасности и удобства современной жизни в самых разных ее областях. Обобщенно такие технологии идентификации человека называются биометрическими.

Биометрия представляет собой совокупность автоматизированных методов и средств идентификации человека, основанных на его физиологической или поведенческой характеристике. Все системы биометрической идентификации выполняют две основные функции.

Регистрация. По нескольким измерениям со считывающего биометрического устройства формируется цифровое представление (шаблон или модель) биометрической характеристики (в зависимости от метода: отпечаток пальца, рисунок радужной оболочки и т. д.), соответствующей регистрируемому человеку.

Идентификация. Одно или большее количество измерений биометрической характеристики со считывающего устройства преобразуется в пригодную для использования цифровую форму и затем сравнивается с единственным шаблоном, соответствующим проверяемому человеку, или со всеми зарегистрированными шаблонами (без предварительного выбора шаблона и ввода номера или кода).

В терминологии идентификация/ аутентификация в настоящее время существует некоторая путаница. В российской литературе по безопасности эти понятия жестко разделены: идентификация - это проверка наличия предъявляемого идентификатора (обычно имени пользователя) в списке зарегистрированных, аутентификация - это проверка принадлежности пользователю (человеку) предъявленного им идентификатора. В иностранной литературе вся процедура проверки имени/пароля может называться как идентификацией, так и аутентификацией. С другой стороны, в литературе по биометрии под идентификацией часто понимается сравнение «один ко многим», то есть аутентификация

В первом случае шаблон выбирается по предварительно вводимому номеру или коду. Результаты сравнения возвращаются приложению: такая процедура называется верификацией или сравнением «один к одному». Результатом сравнения обычно является число - вероятность того, что сравниваемые шаблоны принадлежат одному лицу. Затем с использованием какого-либо математического критерия принимается решение об идентичности шаблонов.

Во втором - в качестве результата возвращается список нескольких наиболее похожих шаблонов (с наибольшими вероятностями, полученными при сравнении). Затем, как и в предыдущем случае, с использованием какого-либо математического критерия принимается решение об идентичности шаблонов. Такая процедура называется аутентификацией или сравнением «один ко многим».

Методы биометрической идентификации делятся на две большие группы:

- статические методы, которые основываются на физиологической (статической) характеристике человека, то есть уникальном свойстве, данном ему от рождения и неотъемлемом от него;
- динамические методы, которые основываются на поведенческой, (динамической) характеристике человека - особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия (подписи, речи, динамики клавиатурного набора).

Рассмотрим наиболее распространенные методы биометрической идентификации и выделим ведущих производителей в каждой из этих областей.

Распознавание по отпечаткам пальцев. Это - самый распространенный статический метод биометрической идентификации, в основе которого лежит уникальность для каждого человека рисунка папиллярных узоров на пальцах. Изображение отпечатка пальца, полученное с помощью специального сканера, преобразуется в цифровой код (свертку) и сравнивается с ранее введенным шаблоном (эталоном) или набором шаблонов (в случае аутентификации).

Ведущие производители оконечного оборудования (сканеров отпечатков пальцев):

- BioLink, **www.biolink.ru**, **www.biolinkusa.com**;
- Bioscrypt, **www.bioscrypt.com**;
- DigitalPersona, **www.digitalpersona.com**;
- Ethentica, **www.ethentica.com**;
- Identix, **www.identix.com**;
- Precise Biometrics, **www.precisebiometrics.com**;
- Saflink, **www.saflink.com**.

Ведущие производители сенсоров (считывающих элементов для сканирующих устройств):

- Atmel, **www.atmel.com**, **www.atmel-grenoble.com**;
- AuthenTec, **www.authentec.com**;
- Veridicom, **www.veridicom.com**;
- Fujitsu, **www.fujitsu.com**.

Распознавание по форме руки. Данный статический метод построен на распознавании геометрии кисти руки, также являющейся уникальной биометрической характеристикой человека. С помощью специального устройства, позволяющего получать трехмерный образ кисти руки (некоторые производители сканируют форму нескольких пальцев), получаются измерения, необходимые для получения уникальной цифровой свертки, идентифицирующей человека.

Ведущие производители:

- Recognition Systems, **www.recogsys.com**, **www.recogsys.com**;
- BioMet Partners, **www.biomet.ch**.

Распознавание по радужной оболочке **глаза.** Этот метод распознавания основан на уникальности рисунка радужной оболочки глаза. Для реализации метода необходима камера, позволяющая получить изображение глаза человека с достаточным разрешением, и специализированное программное обеспечение, позволяющее выделить из полученного изображения рисунок радужной оболочки глаза, по которому строится цифровой код для идентификации человека.

Ведущие производители:

- Iridian — крупнейший производитель в данной области, на решениях этой компании базируются практически все разработки других: LG, Panasonic, OKI, Saflink и т. д., **www.iridiantech.com**.

Распознавание по форме лица. В данном статическом методе идентификации строится двух- или трехмерный образ лица человека. С помощью камеры и специализированного программного обеспечения на изображении или наборе изображений лица выделяются контуры бровей, глаз, носа, губ и т. д., вычисляются расстояния между ними и другие параметры, в зависимости от используемого алгоритма. По этим данным строится образ, преобразуемый в цифровую форму для сравнения. Причем количество, качество и разнообразие (разные углы поворота головы, изменения нижней части лица при произношении ключевого слова и т. д.) считываемых образов может варьироваться в зависимости от алгоритмов и функций системы, реализующей данный метод.

Ведущие производители:

- AcSys Biometrics, **www.acsysbiometrics.com** ;
- A4Vision, **www.a4vision.com**;
- Cognitec Systems, **www.cognitecsystems.de** , **www.cognitec.com**;
- Identix (в 2002 году в состав компании вошел один из лидеров в данной области Visionics), **www.identix.com**;
- Imagis, **www.imagistechnologies.com** ;
- Vicar Vision, **www.vicarvision.nl**;
- ZN Vision, **www.zn-ag.com**.

Распознавание по рукописному почерку. Как правило, для этого динамического метода идентификации человека используется его подпись (иногда написание кодового слова). Цифровой код идентификации формируется по динамическим характеристикам написания, то есть для идентификации строится свертка, в которую входит информация по графическим параметрам подписи, временным характеристикам нанесения подписи и динамики нажима на поверхность в зависимости от возможностей оборудования (графический планшет, экран карманного компьютера и т. д.).

Ведущие производители:

- CIC (Communication Intelligence Corporation), **www.cic.com**;
- Cyber-SIGN, **www.cybersign.com**;
- SOFTPRO, **www.signplus.com**;
- Valyd, **www.valyd.com**.

Распознавание по клавиатурному почерку. Метод в целом аналогичен вышеописанному, однако вместо подписи в нем используется некое кодовое слово, а из оборудования требуется только стандартная клавиатура. Основная характеристика, по которой строится свертка для идентификации, - динамика набора кодового слова.

Ведущие производители:

- BioPassword Security Software, **www.biopassword.com**;
- Checco, **www.biochec.com**.

Распознавание по голосу. В настоящее время развитие этой одной из старейших технологий ускорилось, так как предполагается ее широкое использование при сооружении интеллектуальных зданий. Существует достаточно много способов построения кода идентификации по голосу: как правило, это различные сочетания частотных и статистических характеристик последнего.

Ведущие производители:

- Nuance, **www.nuance.com**;
- Persay, **www.persay.com**;
- Voicevault, **www.voicevault.com**.

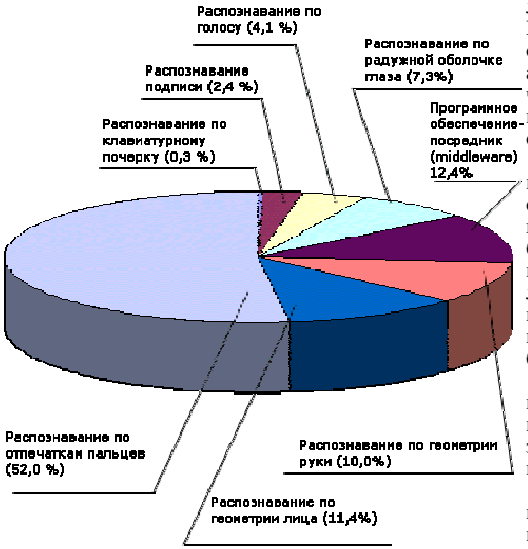
Существует еще множество других, как уже неиспользуемых, так и перспективных, например: по термографии лица, по расположению вен на запястье, по динамике поворота ключа в дверном замке и т. д.

Общей характеристикой, используемой для сравнения различных методов и способов биометрической идентификации, являются статистические показатели: ошибка первого рода (отвергнуть «своего») и ошибка второго рода (пропустить «чужого»).

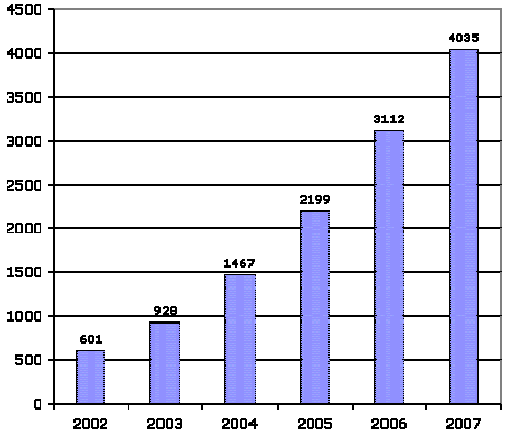
Сортировать и сравнивать описанные выше биометрические методы по показаниям ошибок первого и второго рода очень сложно, так как они сильно разнятся для одних и тех же методов из-за сильной зависимости от оборудования, на котором они реализованы.

Кроме описанных выше производителей в настоящее время на рынке биометрии появилась новая группа компаний, решения которых называются middleware. Как правило, это «программное обеспечение -посредник» между оконечным оборудованием и программными системами, в которые интегрируются процедуры биометрической идентификации. Причем middleware может реализовать как просто вход в систему с использованием измерений биометрического сканера (например, Windows Logon), так и самостоятельный функционал, например создание криптографических контейнеров с помощью ключа, получаемого только по определенному отпечатку пальца.

Рассмотрим сегментацию рынка биометрических технологий. По данным ведущей в данной области консалтинговой компании International Biometric Group лидирующее положение с огромным отрывом занимает технология аутентификации по отпечаткам пальцев. Причем, как видно из рисунка, в данных IBG сегмент middleware выделен в самостоятельную область.



Сегментация рынка по данным International Biometric Grou



Объем рынка биометрических технологий по данным International Biometric Group в период с 2002 по 2007 гг. (в млн долл.)

Технология распознавания по отпечатку пальца лидирует. Объясняется это в первую очередь универсальностью данной технологии, которую, в отличие от остальных методов биометрической идентификации, можно использовать для решения задач в самых различных областях от систем контроля доступа и учета рабочего времени до идентификации в мобильных телефонах и системах автомобильной сигнализации.

Объем биометрического рынка также с каждым годом меняется, причем меняются и прогнозы на его развитие. Продемонстрируем это также на примерах оценок, даваемых ABI и IBG.

Прогноз, данный IBG, предполагал постепенное развитие биометрического рынка с выходом общего объема к 2007 году на отметку в 4 млрд долл.

Такое различие в прогнозах объясняется во многом следующим фактом: несмотря на 20-летний стаж развития биометрии как отдельной области в информационной безопасности, резкий скачок интереса к ней произошел только в 2001 году после трагических событий в США 11 сентября. Следствием этих событий стало сокращение времени на адаптацию технологии в различных областях применения. В первую очередь эти изменения коснулись систем проверки личности на стратегических объектах и регистрации в различных государственных системах идентификации (визовых, миграционных службах, силовых министерствах и ведомствах и т. д.). Наибольший интерес был обращен к технологиям идентификации по форме лица, радужной оболочке глаза и отпечаткам пальцев.

Вследствие этого, на рынке биометрических продуктов, насчитывавшем ранее около 50 компаний, наряду с признанными лидерами биометрии появились новые игроки - крупные компании, ранее не специализировавшиеся в данной области: Sony, Sanyo, ActivCard, LG, Compaq, Polaroid, NEC, Panasonic и другие. Они поглотили часть старожилов и теперь продвигают новые для себя технологии во всех своих решениях. Это влечет за собой серьезное расширение сферы использования биометрии и свидетельствует о том, что в скором будущем она станет частью нашей обыденной жизни.

Еще одним показателем развития биометрии является стандартизация данной области. Причем стандартизация идет по нескольким направлениям: как для отдельных областей, так и для всех методов биометрической идентификации в целом. Как правило, в них определяется единый формат представления биометрических данных, API, определяющий единый алгоритм работы систем биометрической идентификации и необходимые для этого функции, возможности взаимодействия с другими технологиями идентификации (в первую очередь карточными), различными криптографическими системами, а также правила использования в различных областях, таких как электронные платежи, ЭЦП, идентификация через Интернет.

Разработкой стандартов по биометрии занимаются государственные структуры, международные организации по стандартизации и независимые консорциумы, являющиеся объединением нескольких производителей.

Наиболее распространенными (или планируемыми к широкому распространению) являются следующие стандарты: BioAPI, BAPI, CDSA/HRS, CBEFF, X9.84, ANSI/ NIST ITL 2000, ANSI B10.8, ICAO (SC17). С их содержанием можно ознакомиться на сайтах соответствующих организаций или заказать их через Интернет.

В заключение хотелось бы сказать о ближайших перспективах развития биометрии. Судя по всему, доминирующим методом идентификации по-прежнему останется распознавание отпечатков пальцев. Стоит выделить две главные причины этого:

- в нескольких странах дан старт многолетним государственным проектам построения системы идентификации по отпечаткам пальцев и переходу на паспорта, содержащие биометрические данные (в некоторых государствах в такие паспорта планируется вносить несколько биометрических характеристик, кроме отпечатков пальцев, например, свертку сетчатки глаза и формы лица);
- появляются новые типы сканеров отпечатков пальцев: в этом году появилось два вида «узких» сканеров (длина сканирующей поверхности от 3 до 5 мм) - полупроводниковый прокаточный сканер (sweep) и прокруточный оптический сканер, размеры которых позволяют использовать их в мобильных устройствах маленьких размеров (например, в сотовых телефонах, ноутбуках, карманных ПК).

Значительное расширение может ожидать сектор идентификации по подписи, так как в связи с повсеместным внедрением ЭЦП эта технология распознавания может быть легко интегрирована в карманные ПК и другие мобильные вычислительные средства, предоставляющие возможность нанесения рукописной подписи. Распознавание голоса, возможно, наберет ожидаемые обороты в связи с реализацией нескольких крупных проектов в области строительства интеллектуальных зданий.

Таким образом, можно резюмировать, что развитие биометрии продолжается, рынок биометрических средств защиты растет, и в ближайшее время нас ожидает множество интересных новинок и новостей, связанных с развитием биометрических технологий.

Аппаратно-программные средства контроля доступа

На мировом рынке информационной безопасности стабильно развиваются так называемые средства AAA (от англ. authentication, authorization, administration — аутентификация, авторизация, администрирование), предназначенные для защиты от несанкционированного доступа (НСД) к информационным ресурсам автономных и сетевых компьютеров. Согласно прогнозам **Infonetics Research** рынок средств AAA к 2005 г. составит примерно 9,5 млрд. долл., или 67% от всего рынка информационной безопасности. Этот прогноз не вызывает удивления, ведь известно, что основной ущерб предприятиям вследствие нарушений политики безопасности наносят злоупотребления со стороны собственных недобросовестных сотрудников. Как показывают исследования компании **Ernst & Young**, 80% случаев потерь конфиденциальной информации приходится именно на внутрикорпоративные угрозы и только 20% — на внешние.

Среди средств AAA важное место занимают аппаратно-программные инструменты контроля доступа к компьютерам — электронные замки, устройства ввода идентификационных признаков (УВИП) и соответствующее ПО. Совместное применение УВИП и электронного замка дает возможность воздвигнуть перед злоумышленником две линии обороны, преодолеть которые не так-то просто. Разумеется, речь здесь не идет о физическом взломе компьютера.

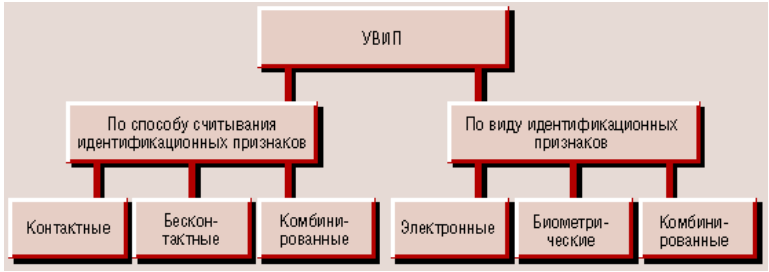
Две линии обороны — УВИП и электронный замок

Доступ к информационным ресурсам компьютера пользователь получает после успешного выполнения процедур идентификации и аутентификации. Идентификация заключается в распознавании пользователя по присущему или присвоенному ему идентификационному признаку. Проверка принадлежности предъявленного им идентификатора (подтверждение подлинности) проводится в процессе аутентификации.

В аппаратно-программных средствах контроля доступа к компьютерам идентификация и аутентификация, а также ряд других важных защитных функций, которые описываются ниже, осуществляются с помощью электронного замка и УВИП до загрузки ОС.

Устройства ввода идентификационных признаков

В состав аппаратных средств УВИП входят идентификаторы и считывающие устройства (иногда считыватели могут отсутствовать). Современные УВИП принято классифицировать по виду идентификационных признаков и по способу их считывания.



Классификация УВИП

По способу считывания они подразделяются на контактные, дистанционные (бесконтактные) и комбинированные.

Контактное считывание идентификационных признаков предполагает непосредственное взаимодействие идентификатора и считывателя — проведение идентификатора через считыватель или их простое соприкосновение.

Бесконтактный (дистанционный) способ считывания не требует четкого позиционирования идентификатора и считывателя. Для чтения данных нужно либо на определенное расстояние поднести идентификатор к считывателю (радиочастотный метод), либо оказаться с ним в поле сканирования считывающего устройства (инфракрасный метод).

Комбинированный способ подразумевает сочетание обоих методов считывания.

По виду используемых идентификационных признаков УВИП могут быть электронными, биометрическими и комбинированными.

В электронных УВИП идентификационные признаки представляются в виде кода, записанного в электронную микросхему памяти идентификатора.

В биометрических устройствах идентификационными признаками являются индивидуальные физические признаки человека (отпечатки пальцев, геометрия ладони, рисунок сетчатки глаза, голос, динамика подписи и т. д.).

В комбинированных УВИП для идентификации используется несколько идентификационных признаков одновременно.

На российском рынке компьютерной безопасности предлагаются разнообразные УВИП. К сожалению, изделия отечественной разработки занимают на нем незначительную часть. Рассмотрим основные, самые распространенные типы устройств.

iButton

Разработанное компанией Dallas Semiconductor устройство ввода идентификационных признаков на базе идентификатора **iButton** относится к классу электронных контактных УВИП.

Модельный ряд идентификаторов iButton довольно широк и разнообразен (более 20 моделей). В общем виде iButton представляет собой микросхему, вмонтированную в герметичный стальной корпус. Корпус отдаленно напоминает батарейку для наручных часов и имеет диаметр 17,35 мм при высоте 5,89 мм (корпус F5) или 3,1 мм (корпус F3).

Идентификатор iButton

Он защищает и обеспечивает высокую степень защищенности идентификатора от воздействия агрессивных сред, пыли, влаги, внешних электромагнитных полей, механических ударов и т. п. Идентификатор легко крепится на носителе (карточке, брелоке).

Обмен информацией идентификатором и компьютером происходит в соответствии с протоколом 1-Wire с помощью разнообразных считывающих устройств (адаптеров последовательного, параллельного и USB-портов, контактных устройств Touch Probe). Для записи и считывания данных из идентификатора нужно, чтобы корпус iButton соприкоснулся со считывающим устройством. Время контакта — не более 5 мс, гарантированное количество контактов составляет несколько миллионов. Интерфейс 1-Wire обеспечивает обмен информацией на скоростях 16 кбит/с или 142 кбит/с (ускоренный режим).

Для защиты от НСД существует несколько модификаций идентификаторов семейства DS199X, которые различаются емкостью памяти, функциональными возможностями и соответственно ценой. Ориентировочная цена идентификаторов iButton на российском рынке в зависимости от типа составляет от 2 до 12, контактных устройств — от 5 до 12 долл.

ТИП ИЗДЕЛИЯ	ЕМКОСТЬ NV RAM, КБИТ	ЕМКОСТЬ SM, БИТ	ЕМКОСТЬ ПЗУ, БАЙТ	КОНСТРУКЦИЯ КОРПУСА
DS1996	64	256	64	F5
DS1995	16	256	64	F5
DS1994	4	256	64	F5
DS1993	4	256	64	F5
DS1992	1	256	64	F5
DS1991	0,5	512	64	F5
DS1990	—	—	64	F3/F5

Идентификаторы iButton

В структуре iButton можно выделить следующие основные части: постоянное запоминающее устройство (ПЗУ), энергонезависимое (nonvolatile — NV) ОЗУ, сверхоперативное запоминающее устройство (scratchpad memory — SM), часы реального времени (для DS1994), а также элемент питания — встроенную миниатюрную литиевую батарейку. Изделие DS1990 содержит только ROM.

В ПЗУ идентификаторов хранится 64-разрядный код — он состоит из 8-разрядного кода типа идентификатора, 48-разрядного уникального серийного номера и 8-разрядной контрольной суммы.

К достоинствам УВИП на базе электронных ключей iButton относятся:

- надежность, долговечность (время хранения информации в памяти идентификатора составляет не менее 10 лет);
- высокая степень механической и электромагнитной защищенности;
- малые размеры;
- относительно невысокая стоимость.

Недостатком этого устройства является зависимость его срабатывания от точности ручного соприкосновения идентификатора и считывателя, осуществляемого вручную.

Proximity

Устройства ввода идентификационных признаков на базе идентификаторов Proximity (от англ. proximity — близость, соседство) или RFID-системы (radio-frequency identification — радиочастотная идентификация) относятся к классу электронных бесконтактных радиочастотных устройств.

Радиочастотные идентификаторы выпускаются в виде карточек, брелоков, браслетов, ключей и т. п. Каждый из них имеет собственный уникальный серийный номер. Основными их компонентами являются интегральная микросхема, осуществляющая связь со считывателем, и встроенная антенна. В состав микросхемы входят приемо-передатчик и запоминающее устройство, хранящее идентификационный код и другие данные. Внутри Proximity может находиться источник питания — литиевая батарея. Такие идентификаторы называются активными. Они обеспечивают взаимодействие со считывателем на значительном расстоянии (в несколько метров). Дистанция считывания для пассивных идентификаторов (не имеющих батареи) измеряется десятками сантиметров.

Считывающее устройство постоянно излучает радиосигнал. Когда идентификатор оказывается на определенном расстоянии от считывателя, антенна поглощает сигнал и передает его на микросхему. Получив энергию, идентификатор излучает идентификационные данные, принимаемые считывателем. Дистанция считывания в значительной степени зависит от характеристик антенного и приемо-передающего трактов считывателя. Весь процесс занимает несколько десятков микросекунд.

Устройство чтения может размещаться внутри корпуса компьютера. Взаимная ориентация идентификатора и считывателя не имеет значения, а ключи и другие предметы, находящиеся в контакте с картой, не мешают передаче информации.

В соответствии с используемой несущей частотой RFID-системы классифицируются по частоте:

- низкочастотные (100—500 кГц) характеризуются незначительным расстоянием считывания (десятки сантиметров). Идентификационный код считывается через одежду, сумки, портмоне и т. п.;
- устройства промежуточной частоты (10—15 МГц) способны передавать значительные объемы данных;
- высокочастотные (850—950 МГц или 2,4—5 ГГц) характеризуются большой дистанцией считывания (в несколько метров).

На мировом рынке информационной безопасности существует немало фирм, занимающихся разработкой RFID-технологий. Лидерами являются **EM-Marin**, **HID** и **Motorola Indala**. Среди отечественных производителей можно отметить **ОАО "Ангстрем"**, компании **Parsec** и **PERCo**.

Основными достоинствами УВИП на базе идентификаторов Proximity являются:

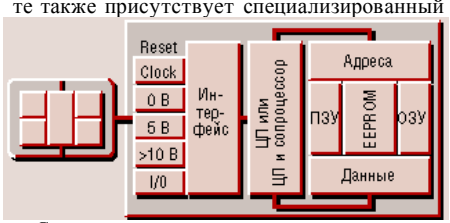
- бесконтактная технология считывания;
- долговечность пассивных идентификаторов (некоторые фирмы-производители дают на карты пожизненную гарантию);
- точность, надежность и удобство считывания идентификационных признаков.

К недостаткам RFID-систем относят слабую электромагнитную защищенность и высокую стоимость (на отечественном рынке идентификаторы в зависимости от типа стоят от 1,3 до 5 долл., цена считывателей может превышать $150).

Устройства ввода на базе смарт-карт

Устройства ввода идентификационных признаков на базе смарт-карт относятся к классу электронных устройств. Они могут быть контактными и бесконтактными (дистанционными).

Основой внутренней организации смарт-карты является так называемая SPOM-архитектура (Self Programming One-chip Memory), предусматривающая наличие центрального процессора (CPU), ОЗУ, ПЗУ и электрически перепрограммируемой постоянной памяти EEPROM. Как правило, в карте также присутствует специализированный сопроцессор.



Структура контактной смарт-карты

Процессор обеспечивает разграничение доступа к хранящейся в памяти информации, обработку данных и реализацию криптографических алгоритмов (совместно с сопроцессором). В ПЗУ хранится исполняемый код процессора, оперативная память используется в качестве рабочей, EEPROM необходима для хранения изменяемых данных владельца карты.

В структуру бесконтактных смарт-карт на базе стандарта MIFARE 1 S50 IC (или MIFARE Standard) дополнительно входит радиочастотный модуль со встроенной антенной, необходимой для связи со считывателем и питания микросхемы. Смарт-карта является пассивной, расстояние считывания составляет не более 10 см. Обмен информацией осуществляется на частоте 13,56 МГц с максимальной скоростью 106 кбит/с.

Каждая смарт-карта обладает собственным уникальным серийным номером. Он задается на заводе-изготовителе, его нельзя изменить на протяжении всего срока эксплуатации карты. Идентификация по серийному номеру, шифрование данных и аутентификация областей памяти с помощью секретных ключей обеспечивают надежную защиту смарт-карт от взлома.

По отношению к компьютеру устройства чтения смарт-карт могут быть внешними и внутренними (например, встроенными в клавиатуру, гнездо 3,5" дисковода, корпус компьютера). Считыватель работает под управлением специальной программы — драйвера устройства чтения.

На базе ISO 7816 разработан единый стандартный интерфейс для работы со смарт-картами. Включенные в него спецификации PC/SC облегчают интеграцию смарт-карт-технологий в программно-аппаратные комплексы на базе платформы персонального компьютера и создание средств разработки приложений для смарт-карт.

На мировом рынке компьютерной безопасности разработкой смарт-карт-технологий занимаются многие фирмы, среди которых выделяются **Bull**, **GemPlus**, **HID**, **Schlumberger**, а также альянс **Fujitsu Siemens Computers**. На отечественном рынке ведущее место занимает **ОАО "Ангстрем"**, разработавшее первую российскую смарт-карту в 1996 г.

Несомненными достоинствами УВИП на базе смарт-карт считаются удобство хранения идентификатора (например, его можно держать в бумажнике вместе с другими карточками) и считывания идентификационных признаков. К недостаткам можно отнести ограниченный срок эксплуатации из-за неустойчивости смарт-карты к механическим повреждениям и высокую стоимость считывателей смарт-карт (на российском рынке ориентировочная цена смарт-карт в зависимости от типа составляет 2—12 долл., а считывателей — более $100).

Устройства ввода на базе USB-ключей

Устройства ввода идентификационных признаков на базе USB-ключей относятся к классу электронных контактных устройств. В составе УВИП данного типа отсутствуют дорогостоящие аппаратные считыватели. Идентификатор, называемый USB-ключом, подключается к USB-порту непосредственно или с помощью соединительного кабеля.

Конструктивно USB-ключи выпускаются в виде брелоков, которые легко размещаются на связке с обычными ключами. Брелоки выпускаются в цветных корпусах и снабжаются световыми индикаторами работы. Каждый идентификатор имеет собственный уникальный серийный номер. Основными компонентами USB-ключей являются встроенные процессор и память. Процессор выполняет функции криптографического преобразования информации и USB-контроллера. Память предназначается для безопасного хранения ключей шифрования, цифровых сертификатов и любой другой важной информации. Поддержка спецификаций PC/SC позволяет без труда переходить от смарт-карт к USB-ключам и встраивать их как в существующие приложения, так и в новые.

Идентификатор eToken R2

На российском рынке безопасности предлагаются следующие USB-ключи:

- серии iKey 10xx и iKey 20xx (разработка компании **Rainbow Technologies**);
- eToken R2, eToken Pro (**Aladdin Knowledge Systems**);
- ePass1000 и ePass2000 (**Feitian Technologies**);
- WebIdentity, CryptoIdentity (**Eutron**).

В табл. представлены некоторые характеристики USB-ключей.

ИЗДЕЛИЕ	ЕМКОСТЬ ПАМЯТИ, Кб	РАЗРЯДНОСТЬ СЕРИЙНОГО НОМЕРА	АЛГОРИТМ ШИФРОВАНИЯ
eToken R2	16/32/64	32	DESX (ключ 120 бит), MD5
eToken Pro	16/32	32	RSA/1024, DES, 3DES (TripleDES), SHA-1
iKey 10xx	8/32	64	DES (режимы ECB и CBC), DES, 3DES, RC2, RC4, RC5, MD5
iKey 20xx	8/32	64	DES (режимы ECB и CBC), DESX, 3DES, RC2, RC4, RC5, RSA/1024
ePass1000	8/32	64	MD5, MD5-HMAC
ePass2000	16/32	64	RSA, DES, 3DES, DSA, MD5, SHA-1
WebIdentity	16/32	32	3DES, MD5
CryptoIdentity	32	32	RSA/1024

Характеристики USB-ключей

Достоинства УВИП на базе USB-ключей заключаются в отсутствии аппаратного считывателя, малых размерах и удобстве хранения идентификаторов, а также в простоте подсоединения идентификатора к USB-порту.

К недостаткам можно отнести сравнительно высокую стоимость (на российском рынке цена USB-ключей в зависимости от типа превышает $20) и слабую механическую защищенность брелока.

Биометрические устройства ввода

Биометрические УВИП относятся к классу электронных устройств (см. PC Week/RE, № 7/2003, с. 24). Они могут быть контактными и бесконтактными (дистанционными).

В основе биометрической идентификации и аутентификации лежит считывание и сравнение предъявляемого биометрического признака пользователя с имеющимся эталоном. Такого рода признаки включают в себя отпечатки пальцев, форму и термограмму лица, рисунок сетчатки и радужной оболочки глаза, геометрию руки, узор, образуемый кровеносными сосудами ладони человека, речь и т. д. Высокий уровень защиты определяется тем, что биометрия позволяет идентифицировать человека, а не устройство.

До недавнего времени широкое использование биометрических УВИП в средствах контроля доступа к компьютерам тормозилось их высокой ценой. Успехи в технологиях, теории распознавания и микроэлектронике позволили разработчикам снизить стоимость устройств и тем самым активизировать рынок.

Особенно эта тенденция характерна для устройств дактилоскопического доступа. Отпечаток пальца считается одним из наиболее устойчивых идентификационных признаков (не изменяется со временем, при повреждении кожного покрова идентичный папиллярный узор полностью восстанавливается, при сканировании не вызывает дискомфорта у пользователя). Согласно отчету **International Biometric Group** (доля устройств дактилоскопического доступа в 2002 г. составила 52,1% мирового биометрического рынка.

Считыватели (или сканеры) отпечатков пальцев представляют собой подключаемые к одному из портов компьютера отдельные устройства либо они встраиваются в компьютерные мыши, клавиатуры, корпуса мониторов. Наибольшее распространение получили дактилоскопические мыши, ориентировочная цена которых на российском рынке составляет от 75 долл.

Сканирующее устройство и мышь компании SecuGen

Среди устройств дактилоскопического доступа в России наиболее широко представлены мыши Eyed Mouse и Optical Eyed Mouse компании **SecuGen**, U-Match Mouse фирмы **Biolink Technologies International**, ID Mouse корпорации **Siemens AG** и некоторые другие.

Несмотря на тенденцию снижения цены и заявляемые разработчиками отменные характеристики устройств (для Biolink U-Match Mouse вероятность ложного отказа в доступе составляет 10–2, а вероятность ложного доступа — 10–9), ряд экспертов подвергают сомнению высокую эффективность потребительских биометрических УВИП.

Так, в ноябре 2002 г. в немецком компьютерном журнале **c't** была опубликована статья, авторам которой с помощью тривиальных способов удалось обмануть 11 биометрических систем известных компаний, использующих в качестве идентификационных признаков отпечатки пальцев, лицо и радужную оболочку глаза.

Как отмечается в публикации, для обмана УВИП на основе емкостных сенсоров, обладающих эффектом "последействия", достаточно подышать на сенсор или приложить к нему наполненный водой полиэтиленовый пакет. В этом случае восстанавливается отпечаток пальца, оставленный за-

регистрированным пользователем. Есть и более эффективный способ, применимый не только к емкостным сенсорам, — взять отпечаток пальца, оставленного пользователем на какой-нибудь поверхности, и скопировать его с помощью графитовой пудры и липкой ленты. Кроме того, искусственный силиконовый палец позволил одурачить шесть дактилоскопических сканеров, система распознавания по чертам лица была обманута путем демонстрации на мониторе ноутбука видеопортрета ранее зарегистрированного пользователя и т. д.

Комбинированные устройства ввода

Эффективность защиты компьютеров от НСД может быть повышена за счет комбинирования различных УВИП. Эта тенденция наглядно просматривается в изделиях ведущих мировых компаний.

Корпорация **HID** разработала карты-идентификаторы, объединяющие в себе различные технологии считывания идентификационных признаков. Например, в устройстве Smart ISOProx II сочетаются Proximity 125 кГц и контактная смарт-карт-технология MIFARE 13,56 МГц, в HID MIFARE Card — контактные и бесконтактные смарт-карт-технологии. В идентификаторе HID Proximity and MIFARE Card собран букет из трех технологий: Proximity 125 кГц, MIFARE 13,56 МГц и контактная смарт-карта.

Альянс **Fujitsu Siemens Computers** предлагает комбинированное УВИП под названием KBPC-CID. Данное изделие представляет собой объединенные встроенные в клавиатуру компьютера считыватель для смарт-карт и дактилоскопический сканер. Клавиатура подключается к USB-порту защищаемого компьютера.

Изделие KBPC-CID

В компании **Siemens** найдено решение, позволяющее хранить в смарт-карте три биометрических идентификационных признака пользователя: отпечаток пальца, черты лица и голос. Представляется интересным желание объединить USB-ключ с биометрической системой идентификации. Подобное предложение поступило от компании Trekstor, выпустившей изделие **ThumbDrive Touch**. Основными компонентами устройства, выполненного в виде USB-брелока, являются дактилоскопический сканер и энергонезависимая флэш-память емкостью от 32 до 512 Мб. В памяти выделяются открытая и защищенная области. Пользователь получает доступ к защищенной области памяти после проверки отпечатков пальцев. Скорость чтения и записи данных составляет 500 и 250 Кб/с соответственно.

При выборе того или иного комбинированного УВИП следует не забывать известную пословицу: “Где тонко, там и рвется”, — что в переводе на язык теории систем означает: эффективность системы определяется эффективностью самого слабого звена.

Электронные замки

На электронные замки возлагается выполнение следующих защитных функций:

- идентификация и аутентификация пользователей с помощью УВИП;
- блокировка загрузки операционной системы с внешних съемных носителей;
- контроль целостности программной среды компьютера;
- регистрация действий пользователей и программ.

Конструктивно электронные замки выполняются в виде плат расширения, устанавливаемых в разъемы системных шин PCI или ISA. Свои основные функции электронные замки реализуют до загрузки операционной системы компьютера. Для этого в составе каждого изделия имеется собственная память EEPROM, дополняющая базовую систему ввода-вывода BIOS компьютера. При включении компьютера выполняется копирование содержимого EEPROM замка в так называемую теневую область (Shadow Memory) оперативной памяти компьютера, с которой и ведется дальнейшая работа.


Изделие ThumbDrive Touch

На российском рынке разработкой электронных замков занимается ограниченное число фирм. Ниже рассматриваются наиболее известные сертифицированные изделия отечественных компаний.

Российские разработки

Научно-инженерное предприятие **“Информзащита”** выпускает электронные замки “Соболь-PCI” и “Соболь 1.0”. В базовый комплект поставки каждого изделия входят плата электронного замка, контактное считывающее устройство и два идентификатора iButton, интерфейсные кабели, блокирующие загрузку ОС с внешних носителей, и программное обеспечение. Плата электронного замка “Соболь-PCI” устанавливается в разъем системной шины PCI, а плата “Соболя 1.0” — в разъем ISA. Контактное устройство может подключаться как к внешнему, так и к внутреннему разъемам платы.

Электронный замок “Соболь-PCI”

На платах электронных замков размещаются микросхемы энергонезависимой памяти, перепрограммируемая логическая матрица, встроенный датчик случайных чисел, реле аппаратной блокировки устройств. При каждом включении компьютера автоматически проверяется работоспособность датчика случайных чисел.

Идентификация пользователя осуществляется с помощью УВИП на базе iButton. Скорость обмена данными между персональным идентификатором и платой замка составляет 16 кбит/с. Для авторизации применяется пароль и персональный идентификатор. В электронном замке поддерживается работа с паролями длиной до 16 символов.

Запрет загрузки ОС с внешних носителей (магнитных, оптических и магнитно-оптических дисков) возможен программным и аппаратным способами путем блокировки доступа к устройствам чтения при запуске компьютера. После успешной загрузки ОС доступ восстанавливается с помощью специальной программы, входящей в состав электронного замка.

Контроль целостности программной среды компьютера заключается в проверке изменения файлов и секторов жесткого диска. Для этого вычисляются некоторые текущие контрольные значения проверяемых объектов и сравниваются с заранее рассчитанными эталонными.

Электронные замки устанавливаются в компьютеры, функционирующие под управлением операционных систем MS- DOS, Windows, UNIX, FreeBSD.

Электронный замок “Соболь-PCI” сертифицирован ФАПСИ и Гостехкомиссией при Президенте РФ, изделие “Соболь 1.0” — ФАПСИ России.

Замки “Соболь-PCI” и “Соболь 1.0” в комплекте с двумя идентификаторами iButton DS1992, внешним считывателем Touch Probe, двумя интерфейсными кабелями для аппаратной блокировки внешних носителей стоят соответственно 230 и 190 долл.

Особое конструкторское бюро систем автоматизированного проектирования и фирма “ИнфоКрипт” совместно разработали программно-аппаратный комплекс средств защиты информации от НСД “Аккорд-АМДЗ”, который реализуется на базе аппаратных модулей доверенной загрузки — контроллеров “Аккорд-5” (для компьютеров с системной шиной стандарта PCI), “Аккорд-4.5” (для стандарта ISA) и их модификаций.


Контроллер “Аккорд-5”

Термином “доверенная загрузка” разработчики замка определяют случай, когда операционная система загружается только после идентификации и аутентификации пользователя, а также проверки целостности технических и программных средств компьютера. Контроллеры “Аккорд-5” и “Аккорд 4.5” обеспечивают режим доверенной загрузки для операционных систем MS-DOS, Windows, OS/2, UNIX FreeBSD.

Резидентное ПО замков (средства администрирования, идентификации и аутентификации, поддержки контроля целостности, журнал регистрации) размещается в энергонезависимой памяти контроллеров. Электронные замки комплектуются неконтролируемыми аппаратными датчиками случайных чисел.

Для идентификации пользователя применяется УВИП на базе iButton. Аутентификация осуществляется по паролю, вводимому пользователем с клавиатуры. В электронном замке поддерживается работа с паролями длиной до 12 символов.

Помимо традиционного контроля целостности программной среды электронные замки “Аккорд-АМДЗ” обеспечивают проверку целостности технических средств защищаемого компьютера, что немаловажно при отсутствии контроля над физической целостностью корпуса компьютера.

Контроллеры могут функционировать вместе со специальным программным обеспечением, реализующим алгоритмы разграничения доступа пользователей и размещаемым на жестком диске.

Электронные замки “Аккорд-АМДЗ” на базе контроллеров “Аккорд-5” и “Аккорд-4.5” сертифицированы ФАПСИ России и Гостехкомиссией при Президенте РФ.

Цена этих контроллеров в комплекте с двумя идентификаторами iButton DS1992, внешним считывателем с фиксатором DS-13, двумя устройствами блокировки физических каналов составляет 309 и 247 долл. соответственно.

Концерн **“Системпром”** выпускает аппаратно-программные средства криптографической защиты информации М-502 и “Щит”, относящиеся к электронным замкам класса КЭЗ-1.99 в соответствии с требованиями ФАПСИ. Различаются они тем, что М-502 можно использовать при обработ-

ке данных, составляющих государственную тайну, а “Щит” — при обработке данных, не составляющих государственной тайны.

Электронный замок “Щит”

Оба изделия обладают стандартным набором функций электронных замков (идентификация и аутентификация, запрет загрузки операционной системы с внешних устройств, контроль целостности файлов и загрузочных секторов жесткого диска, регистрация событий, связанных с безопасностью). Платы замков устанавливаются в разъем системной шины ISA.

Идентификация осуществляется с помощью электронной карты M64 с открытой памятью на 64 кбит, аутентификация — посредством ввода пароля с клавиатуры компьютера.

Электронные замки М-502 и “Щит” сертифицированы ФАПСИ. Их цена составляет $250.

Фирма **“Анкад”** известна своими аппаратными шифраторами серии “Криптон”, выпускаемыми в виде плат расширения системных шин PCI или ISA. Желая защитить компьютеры от НСД, разработчики создали устройства, позволяющие дополнительно реализовать часть функций электронных замков: идентификацию и аутентификацию пользователей, контроль целостности программной среды компьютера. Эти изделия (“Криптон-замок”, “Криптон-4К/16 замок” — для разъема ISA; “Криптон-4/PCI”, “Криптон-8/PCI” — для разъема PCI) получили общее название — устройства криптографической защиты данных и ограничения доступа к компьютеру.

Идентификация пользователей осуществляется с помощью электронных карт с открытой либо защищенной памятью, смарт-карт, идентификаторов iButton DS1993 и DS1994. Для чтения содержимого карт используются считыватель SR-210 или адаптер SA-101i, которые устанавливаются в свободный 3,5”-слот.

Контроль целостности ОС и системных областей памяти, а также другого программного обеспечения, размещенного на жестком диске, производится согласно списку, хранящемуся в памяти замка. Список контролируемых файлов хранится вместе с контрольными суммами или хэш-значениями, рассчитанными для каждого файла по алгоритму ГОСТ Р 34.11—94. Если хэш-значение хотя бы одного из файлов списка не совпадает с эталонным, это расценивается как нарушение целостности операционной системы и загрузка компьютера блокируется.

Устройства фирмы “Анкад” работают под управлением операционных систем MS-DOS, Windows 9x NT 4.0. Все события, связанные с их эксплуатацией, фиксируются в журнале регистрации.

Изделие “Криптон-замок” (и его модификация “Криптон-4К/16 замок”) сертифицировано Гостехкомиссией при Президенте РФ.

В комплект поставки устройств криптографической защиты данных и ограничения доступа к компьютеру входят плата, установочная дискета и две дискеты с драйверами и библиотеками функций для операционных систем Windows 9x/NT 4.0. Цена комплекта “Криптон-замок” составляет $149, “Криптон-4/ PCI” — $390, “Криптон-8/PCI” — $799. Устройства ввода идентификационных признаков и соответствующее программное обеспечение в комплект поставки не входят и приобретаются отдельно.

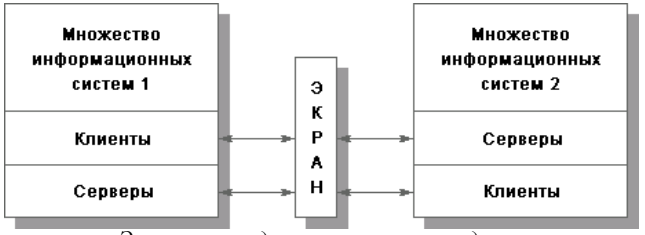
Заключение

Любой здравомыслящий хозяин старается защитить свое жилище от проникновения грабителей. С этой целью, в частности, на входную дверь устанавливается комплект прочных замков. Так неужели компьютеры, содержащие важную и ценную информацию, не нуждаются в надежной защите от возможных нападений недобросовестных сотрудников? Ответ очевиден: нуждаются. И здесь неплохую службу могут сослужить аппаратно-программные средства контроля доступа к компьютерам.

Лекция 11. Экранирование, анализ защищенности

Экранирование. Основные понятия.

Формальная постановка задачи **экранирования** состоит в следующем. Пусть имеется два множества информационных систем. **Экран** - это средство **разграничения доступа** клиентов из одного множества к серверам из другого множества. Экран осуществляет свои функции, контролируя все информационные потоки между двумя множествами систем. Контроль потоков состоит в их **фильтрации**, возможно, с выполнением некоторых преобразований.



Экран как средство разграничения доступа.

На следующем уровне детализации экран (полупроницаемую мембрану) удобно представлять как последовательность **фильтров**. Каждый из фильтров, проанализировав данные, может задержать (не пропустить) их, а может и сразу "перебросить" за экран. Кроме того, допускается преобразование данных, передача порции данных на следующий фильтр для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю.

Экран как последовательность фильтров.

Помимо функций разграничения доступа, экраны осуществляют **протоколирование** обмена информацией.

Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования формулируется как защита внутренней области от потенциально враждебной внешней. Так, **межсетевые экраны (МЭ)** (предложенный автором перевод английского термина firewall) чаще всего устанавливают для защиты корпоративной сети организации, имеющей выход в Internet.

Экранирование помогает поддерживать **доступность** сервисов внутренней области, уменьшая или вообще ликвидируя нагрузку, вызванную внешней активностью. Уменьшается уязвимость внутренних сервисов безопасности, поскольку первоначально злоумышленник должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно. Кроме того, экранирующая система, в отличие от универсальной, может быть устроена более простым и, следовательно, более безопасным образом.

Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима **конфиденциальности** в ИС организации.

Подчеркнем, что экранирование может использоваться как сервис безопасности не только в сетевой, но и в любой другой среде, где происходит обмен сообщениями. Важнейший пример подобной среды - объектно-ориентированные программные системы, когда для активизации методов объектов выполняется (по крайней мере, в концептуальном плане) передача сообщений. Весьма вероятно, что в будущих объектно-ориентированных средах экранирование станет одним из важнейших инструментов разграничения доступа к объектам.

Экранирование может быть частичным, защищающим определенные информационные сервисы. Экранирование электронной почты описано в статье "Контроль над корпоративной электронной почтой: система "Дозор-Джет"" (Jet Info, 2002, 5).

Ограничивающий интерфейс также можно рассматривать как разновидность экранирования. На невидимый объект трудно нападать, особенно с помощью фиксированного набора средств. В этом смысле Web-интерфейс обладает естественной защитой, особенно в том случае, когда гипертекстовые документы формируются динамически. Каждый пользователь видит лишь то, что ему положено видеть. Можно провести аналогию между динамически формируемыми гипертекстовыми

документами и представлениями в реляционных базах данных, с той существенной оговоркой, что в случае Web возможности существенно шире.

Экранирующая роль **Web-сервиса** наглядно проявляется и тогда, когда этот сервис осуществляет посреднические (точнее, интегрирующие) функции при доступе к другим ресурсам, например таблицам базы данных. Здесь не только контролируются потоки запросов, но и скрывается реальная организация данных.

Архитектурные аспекты

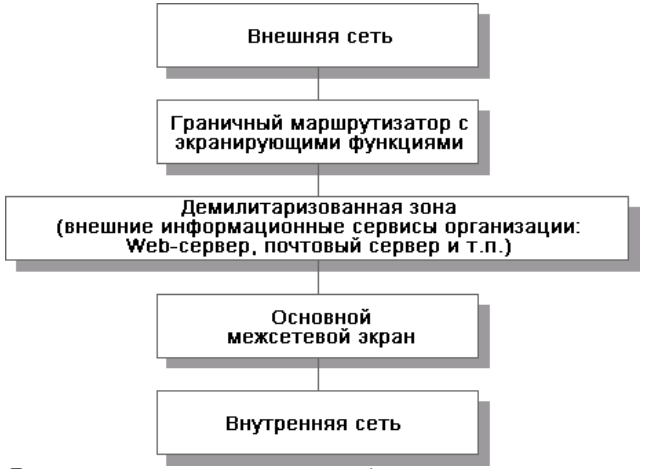
Бороться с угрозами, присущими сетевой среде, средствами универсальных операционных систем не представляется возможным. Универсальная ОС - это огромная программа, наверняка содержащая, помимо явных ошибок, некоторые особенности, которые могут быть использованы для нелегального получения привилегий. Современная технология программирования не позволяет сделать столь большие программы безопасными. Кроме того, администратор, имеющий дело со сложной системой, далеко не всегда в состоянии учесть все последствия производимых изменений. Наконец, в универсальной многопользовательской системе бреши в безопасности постоянно создаются самими пользователями (слабые и/или редко изменяемые пароли, неудачно установленные права доступа, оставленный без присмотра терминал и т.п.). Единственный перспективный путь связан с разработкой специализированных сервисов безопасности, которые в силу своей простоты допускают формальную или неформальную верификацию. Межсетевой экран как раз и является таким средством, допускающим дальнейшую декомпозицию, связанную с обслуживанием различных сетевых протоколов.

Межсетевой экран располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети). В первом случае говорят о внешнем МЭ, во втором - о внутреннем. В зависимости от точки зрения, **внешний межсетевой экран** можно считать первой или последней (но никак не единственной) линией обороны. Первой - если смотреть на мир глазами внешнего злоумышленника. Последней - если стремиться к защищенности всех компонентов корпоративной сети и пресечению неправомерных действий внутренних пользователей.

Межсетевой экран - идеальное место для встраивания средств активного аудита. С одной стороны, и на первом, и на последнем защитном рубеже выявление подозрительной активности по-своему важно. С другой стороны, МЭ способен реализовать сколь угодно мощную реакцию на подозрительную активность, вплоть до разрыва связи с внешней средой. Правда, нужно отдавать себе отчет в том, что соединение двух сервисов безопасности в принципе может создать брешь, способствующую атакам на доступность.

На межсетевой экран целесообразно возложить идентификацию/аутентификацию внешних пользователей, нуждающихся в доступе к корпоративным ресурсам (с поддержкой концепции единого входа в сеть).

В силу принципов **эшелонированности обороны** для защиты внешних подключений обычно используется **двухкомпонентное экранирование**. Первичная фильтрация (например, блокирование пакетов управляющего протокола SNMP, опасного атаками на доступность, или пакетов с определенными IP-адресами, включенными в "черный список") осуществляется **граничным маршрутизатором** (см. также следующий раздел), за которым располагается так называемая **демилитаризованная зона** (сеть с умеренным доверием безопасности, куда выносятся внешние информационные сервисы организации - Web, электронная почта и т.п.) и основной МЭ, защищающий внутреннюю часть корпоративной сети.



Двухкомпонентное экранирование с демилитаризованной зоной.

Теоретически **межсетевой экран** (особенно внутренний) **должен быть многопротокольным**, однако на практике доминирование семейства протоколов TCP/IP столь велико, что поддержка других протоколов представляется излишеством, вредным для безопасности (чем сложнее сервис, тем он более уязвим).

Вообще говоря, и внешний, и **внутренний межсетевой экран** может стать узким местом, поскольку объем сетевого трафика имеет тенденцию быстрого роста. Один из подходов к решению этой проблемы предполагает разбиение МЭ на несколько аппаратных частей и организацию специализированных **серверов-посредников**. Основной межсетевой экран может проводить грубую классификацию входящего трафика по видам и передоверять фильтрацию соответствующим посредникам (например, посреднику, анализирующему HTTP-трафик). Исходящий трафик сначала обрабатывается сервером-посредником, который может выполнять и функционально полезные действия, такие как кэширование страниц внешних Web-серверов, что снижает нагрузку на сеть вообще и основной МЭ в частности.

Ситуации, когда корпоративная сеть содержит лишь один внешний канал, являются скорее исключением, чем правилом. Напротив, типична ситуация, при которой корпоративная сеть состоит из нескольких территориально разнесенных сегментов, каждый из которых подключен к Internet. В этом случае каждое подключение должно защищаться своим экраном. Точнее говоря, можно считать, что корпоративный внешний **межсетевой экран является составным**, и требуется решать задачу согласованного администрирования (управления и аудита) всех компонентов.

Противоположностью составным корпоративным МЭ (или их компонентами) являются **персональные межсетевые экраны и персональные экранирующие устройства**. Первые являются программными продуктами, которые устанавливаются на персональные компьютеры и защищают только их. Вторые реализуются на отдельных устройствах и защищают небольшую локальную сеть, такую как сеть домашнего офиса.

При развертывании межсетевых экранов следует соблюдать рассмотренные нами ранее принципы **архитектурной безопасности**, в первую очередь позаботившись о **простоте** и **управляемости**, об эшелонированности обороны, а также о невозможности **перехода в небезопасное состояние**. Кроме того, следует принимать во внимание не только **внешние**, но и **внутренние угрозы**.

Классификация межсетевых экранов

При рассмотрении любого вопроса, касающегося сетевых технологий, основой служит семиуровневая эталонная модель ISO/OSI. Межсетевые экраны также целесообразно классифицировать по уровню фильтрации - канальному, сетевому, транспортному или прикладному. Соответственно, можно говорить об **экранирующих концентраторах** (мостах, коммутаторах) (уровень 2), маршрутизаторах (уровень 3), о **транспортном экранировании** (уровень 4) и о **прикладных экранах** (уровень 7). Существуют также **комплексные экраны**, анализирующие информацию на нескольких уровнях.

Фильтрация информационных потоков осуществляется межсетевыми экранами на основе **набора правил**, являющихся выражением сетевых аспектов политики безопасности организации. В этих правилах, помимо информации, содержащейся в фильтруемых потоках, могут фигурировать данные, полученные из окружения, например, текущее время, количество активных соединений, **порт**, через который поступил сетевой запрос, и т.д. Таким образом, в межсетевых экранах используется очень мощный логический подход к разграничению доступа.

Возможности межсетевого экрана непосредственно определяются тем, какая информация может использоваться в правилах фильтрации и какова может быть мощность наборов правил. Вообще говоря, чем выше уровень в модели ISO/OSI, на котором функционирует МЭ, тем более содержательная информация ему доступна и, следовательно, тем тоньше и надежнее он может быть сконфигурирован.

Экранирующие маршрутизаторы (и концентраторы) имеют дело с отдельными пакетами данных, поэтому иногда их называют **пакетными фильтрами**. Решения о том, пропустить или задержать

данные, принимаются для каждого пакета независимо, на основании анализа адресов и других полей заголовков сетевого (канального) и, быть может, транспортного уровней. Еще один важный компонент анализируемой информации - порт, через который поступил пакет.

Экранирующие концентраторы являются средством не столько разграничения доступа, сколько оптимизации работы локальной сети за счет организации так называемых виртуальных локальных сетей. Последние можно считать важным результатом применения внутреннего межсетевого экранирования.

Современные маршрутизаторы позволяют связывать с каждым портом несколько десятков правил и **фильтровать пакеты как на входе, так и на выходе**. В принципе, в качестве пакетного фильтра может использоваться и универсальный компьютер, снабженный несколькими сетевыми картами.

Основные достоинства экранирующих маршрутизаторов - доступная цена (на границе сетей маршрутизатор нужен практически всегда, вопрос лишь в том, как задействовать его экранирующие возможности) и **прозрачность** для более высоких уровней модели OSI. Основной недостаток - ограниченность анализируемой информации и, как следствие, относительная слабость обеспечиваемой защиты.

Транспортное экранирование позволяет контролировать процесс установления виртуальных соединений и передачу информации по ним. С точки зрения реализации экранирующий транспорт представляет собой довольно простую, а значит, надежную программу.

По сравнению с пакетными фильтрами, транспортное экранирование обладает большей информацией, поэтому соответствующий МЭ может осуществлять более тонкий контроль за виртуальными соединениями (например, он способен отслеживать количество передаваемой информации и разрывать соединения после превышения определенного порога, препятствуя тем самым несанкционированному экспорту информации). Аналогично, возможно накопление более содержательной регистрационной информации. Главный недостаток - сужение области применения, поскольку вне контроля остаются датаграммные протоколы. Обычно транспортное экранирование применяют в сочетании с другими подходами, как важный дополнительный элемент.

Межсетевой экран, функционирующий на прикладном уровне, способен обеспечить наиболее надежную защиту. Как правило, подобный МЭ представляет собой универсальный компьютер, на котором функционируют **экранирующие агенты**, интерпретирующие протоколы прикладного уровня (HTTP, FTP, SMTP, telnet и т.д.) в той степени, которая необходима для обеспечения безопасности.

При использовании прикладных МЭ, помимо фильтрации, реализуется еще один важнейший аспект экранирования. Субъекты из внешней сети видят только шлюзовой компьютер; соответственно, им доступна только та информация о внутренней сети, которую он считает нужным экспортировать. Прикладной МЭ на самом деле экранирует, то есть заслоняет, внутреннюю сеть от внешнего мира. В то же время, субъектам внутренней сети кажется, что они напрямую общаются с объектами внешнего мира. Недостаток прикладных МЭ - отсутствие полной прозрачности, требующее специальных действий для поддержки каждого прикладного протокола.

Если организация располагает исходными текстами прикладного МЭ и в состоянии эти тексты модифицировать, перед ней открываются чрезвычайно широкие возможности по настройке экрана с учетом собственных нужд. Дело в том, что при разработке систем **клиент/сервер** в многозвенной архитектуре появляются специфические прикладные протоколы, нуждающиеся в защите не меньше стандартных. Подход, основанный на использовании экранирующих агентов, позволяет построить такую защиту, не снижая безопасности и эффективности других приложений и не усложняя структуру связей в межсетевом экране.

Комплексные межсетевые экраны, охватывающие уровни от сетевого до прикладного, соединяют в себе лучшие свойства "одноуровневых" МЭ разных видов. Защитные функции выполняются комплексными МЭ прозрачным для приложений образом, не требуя внесения каких-либо изменений ни в существующее программное обеспечение, ни в действия, ставшие для пользователей привычными.

Комплексность МЭ может достигаться разными способами: "снизу вверх", от сетевого уровня через накопление контекста к прикладному уровню, или "сверху вниз", посредством дополнения прикладного МЭ механизмами транспортного и сетевого уровней.

Помимо выразительных возможностей и допустимого количества правил, качество межсетевого экрана определяется еще двумя очень важными характеристиками - **простотой использования** и **собственной защищенностью**. В плане простоты использования первостепенное значение имеют наглядный интерфейс при определении правил фильтрации и возможность **централизованного администрирования** составных конфигураций. В свою очередь, в последнем аспекте хотелось бы выделить средства централизованной загрузки правил фильтрации и **проверки набора правил на непротиворечивость**. Важен и централизованный сбор и анализ регистрационной информации, а также получение сигналов о попытках выполнения действий, запрещенных политикой безопасности.

Собственная защищенность межсетевого экрана обеспечивается теми же средствами, что и защищенность универсальных систем. Имеется в виду физическая защита, идентификация и аутентификация, разграничение доступа, контроль целостности, протоколирование и аудит. При выполнении централизованного администрирования следует также позаботиться о защите информации от пассивного и активного прослушивания сети, то есть обеспечить ее (информации) целостность и конфиденциальность. Крайне важно оперативное наложение заплат, ликвидирующих выявленные уязвимые места МЭ.

Хотелось бы подчеркнуть, что природа экранирования как сервиса безопасности очень глубока. Помимо блокирования потоков данных, нарушающих политику безопасности, межсетевой экран может скрывать информацию о защищаемой сети, тем самым затрудняя действия потенциальных злоумышленников. Мощным методом сокрытия информации является трансляция "внутренних" сетевых адресов, которая попутно решает проблему расширения адресного пространства, выделенного организации.

Отметим также следующие дополнительные возможности межсетевых экранов:

- контроль информационного наполнения (антивирусный контроль "на лету", верификация Java-апплетов, выявление ключевых слов в электронных сообщениях и т.п.);
- выполнение функций ПО промежуточного слоя.

Особенно важным представляется последний из перечисленных аспектов. ПО промежуточного слоя, как и традиционные межсетевые экраны прикладного уровня, скрывает информацию о предоставляемых услугах. За счет этого оно может выполнять такие функции, как **маршрутизация запросов** и **балансировка нагрузки**. Представляется вполне естественным, чтобы эти возможности были реализованы в рамках межсетевого экрана. Это существенно упрощает действия по обеспечению высокой доступности экспортируемых сервисов и позволяет осуществлять переключение на резервные мощности прозрачным для внешних пользователей образом. В результате к услугам, традиционно предоставляемым межсетевыми экранами, добавляется поддержка высокой доступности сетевых сервисов.

Пример современного межсетевого экрана представлен в статье "Z-2 - универсальный межсетевой экран высшего уровня защиты" (Jet Info, 2002, 5).

Анализ защищенности

Сервис **анализа защищенности** предназначен для выявления уязвимых мест с целью их оперативной ликвидации. Сам по себе этот сервис ни от чего не защищает, но помогает обнаружить (и устранить) пробелы в защите раньше, чем их сможет использовать злоумышленник. В первую очередь, имеются в виду не архитектурные (их ликвидировать сложно), а "оперативные" бреши, появившиеся в результате ошибок администрирования или из-за невнимания к обновлению версий программного обеспечения.

Системы анализа защищенности (называемые также **сканерами** защищенности), как и рассмотренные выше средства активного аудита, основаны на накоплении и использовании знаний. В данном случае имеются в виду знания о пробелах в защите: о том, как их искать, насколько они серьезны и как их устранять.

Соответственно, ядром таких систем является **база** уязвимых **мест**, которая определяет доступный диапазон возможностей и требует практически постоянной актуализации.

В принципе, могут выявляться бреши самой разной природы: наличие вредоносного ПО (в частности, вирусов), слабые пароли пользователей, неудачно сконфигурированные операционные системы, небезопасные сетевые сервисы, неустановленные заплаты, уязвимости в приложениях и т.д. Однако наиболее эффективными являются **сетевые сканеры** (очевидно, в силу доминирования семейства протоколов TCP/IP), а также антивирусные средства. **Антивирусную защиту** мы причисляем к средствам анализа защищенности, не считая ее отдельным сервисом безопасности.

Сканеры могут выявлять уязвимые места как путем пассивного анализа, то есть изучения конфигурационных файлов, задействованных портов и т.п., так и путем имитации действий атакующего. Некоторые найденные уязвимые места могут устраняться автоматически (например, лечение зараженных файлов), о других сообщается администратору.

Системы анализа защищенности снабжены традиционным "технологическим сахаром": **автообнаружением** компонентов анализируемой ИС и графическим интерфейсом (помогающим, в частности, эффективно работать с протоколом сканирования).

С возможностями свободно распространяемого сканера Nessus можно ознакомиться, прочитав статью "Сканер защищенности Nessus: уникальное предложение на российском рынке" (Jet Info, 2000, 10).

Контроль, обеспечиваемый системами анализа защищенности, носит реактивный, запаздывающий характер, он не защищает от новых атак, однако следует помнить, что оборона должна быть эшелонированной, и в качестве одного из рубежей контроль защищенности вполне адекватен. Отметим также, что подавляющее большинство атак носит рутинный характер; они возможны только потому, что известные бреши в защите годами остаются неустраненными.

Безопасность локальных сетей

Крайне важно понять, что безопасность - это не продукт, который можно купить в магазине и быть уверенным в собственной защищенности. "Безопасность" - особая комбинация как технических, так и административных мер. Административные меры также включают в себя не только бумаги, рекомендации, инструкции, но и людей. Невозможно считать свою сеть "безопасной", если вы не доверяете людям, работающим с этой сетью.

Идеальная безопасность - недостижимый миф, который могут реализовать, в лучшем случае, только несколько профессионалов. Есть один фактор, который невозможно преодолеть на пути к идеальной безопасности - это человек.

Основные цели сетевой безопасности

Цели сетевой безопасности могут меняться в зависимости от ситуации, но основных целей обычно три:

Целостность данных.

Конфиденциальность данных.

Доступность данных.

Рассмотрим более подробно каждую из них.

Целостность данных

Одна из основных целей сетевой безопасности - гарантированность того, чтобы данные не были изменены, подменены или уничтожены. Целостность данных должна гарантировать их сохранность как в случае злонамеренных действий, так и случайностей. Обеспечение целостности данных является обычно одной из самых сложных задач сетевой безопасности.

Схема 1. Основные цели сетевой безопасности

Конфиденциальность данных

Второй главной целью сетевой безопасности является обеспечение конфиденциальности данных. Не все данные можно относить к конфиденциальной информации. Существует достаточно большое количество информации, которая должна быть доступна всем. Но даже в этом случае обеспечение целостности данных, особенно открытых, является основной задачей. К конфиденциальной информации можно отнести следующие данные:

- Личная информация пользователей.
- Учетные записи (имена и пароли).
- Данные о кредитных картах.
- Данные о разработках и различные внутренние документы.
- Бухгалтерская информация.

Доступность данных

Третьей целью безопасности данных является их доступность. Бесполезно говорить о безопасности данных, если пользователь не может работать с ними из-за их недоступности. Вот приблизительный список ресурсов, которые обычно должны быть "доступны" в локальной сети:

- Принтеры.
- Серверы.
- Рабочие станции.
- Данные пользователей.
- Любые критические данные, необходимые для работы.

Рассмотрим угрозы и препятствия, стоящие на пути к безопасности сети. Все их можно разделить на две большие группы: технические угрозы и человеческий фактор.

Технические угрозы:

- Ошибки в программном обеспечении.
- Различные DoS- и DDoS-атаки.
- Компьютерные вирусы, черви, троянские кони.
- Анализаторы протоколов и прослушивающие программы ("снифферы").
- Технические средства съема информации.

Ошибки в программном обеспечении

Самое узкое место любой сети. Программное обеспечение серверов, рабочих станций, маршрутизаторов и т. д. написано людьми, следовательно, оно практически всегда содержит ошибки. Чем выше сложность подобного ПО, тем больше вероятность обнаружения в нем ошибок и уязвимостей. Большинство из них не представляет никакой опасности, некоторые же могут привести к трагическим последствиям, таким, как получение злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов (хранение ненужных данных на сервере, использование в качестве плацдарма для атаки и т.п.). Большинство таких уязвимостей

устраняется с помощью пакетов обновлений, регулярно выпускаемых производителем ПО. Своевременная установка таких обновлений является необходимым условием безопасности сети.

DoS- и DDoS-атаки

Denial Of Service (отказ в обслуживании) - особый тип атак, направленный на выведение сети или сервера из работоспособного состояния. При DoS-атаках могут использоваться ошибки в программном обеспечении или легитимные операции, но в больших масштабах (например, посылка огромного количества электронной почты). Новый тип атак DDoS (Distributed Denial Of Service) отличается от предыдущего наличием огромного количества компьютеров, расположенных в большой географической зоне. Такие атаки просто перегружают канал трафиком и мешают прохождению, а зачастую и полностью блокируют передачу по нему полезной информации. Особенно актуально это для компаний, занимающихся каким-либо online-бизнесом, например, торговлей через Internet.

Компьютерные вирусы, троянские кони

Вирусы - старая категория опасностей, которая в последнее время в чистом виде практически не встречается. В связи с активным применением сетевых технологий для передачи данных вирусы все более тесно интегрируются с троянскими компонентами и сетевыми червями. В настоящее время компьютерный вирус использует для своего распространения либо электронную почту, либо уязвимости в ПО. А часто и то, и другое. Теперь на первое место вместо деструктивных функций вышли функции удаленного управления, похищения информации и использования зараженной системы в качестве плацдарма для дальнейшего распространения. Все чаще зараженная машина становится активным участником DDoS-атак. Методов борьбы достаточно много, одним из них является все та же своевременная установка обновлений.

Анализаторы протоколов и "снифферы"

В эту группу входят средства перехвата передаваемых по сети данных. Такие средства могут быть как аппаратными, так и программными. Обычно данные передаются по сети в открытом виде, что позволяет злоумышленнику внутри локальной сети перехватить их. Некоторые протоколы работы с сетью (POPS, FTP) не используют шифрование паролей, что позволяет злоумышленнику перехватить их и использовать самому. При передаче данных по глобальным сетям эта проблема встает наиболее остро. По возможности следует ограничить доступ к сети неавторизированным пользователям и случайным людям.

Технические средства съема информации

Сюда можно отнести такие средства, как клавиатурные жучки, различные мини-камеры, звукозаписывающие устройства и т.д. Данная группа используется в повседневной жизни намного реже вышеперечисленных, так как, кроме наличия спецтехники, требует доступа к сети и ее составляющим.

Человеческий фактор:

- Уволенные или недовольные сотрудники.
- Промышленный шпионаж.
- Халатность.
- Низкая квалификация.

Уволенные и недовольные сотрудники

Данная группа людей наиболее опасна, так как многие из работающих сотрудников могут иметь разрешенный доступ к конфиденциальной информации. Особенную группу составляют системные администраторы, зачастую недовольные своим материальным положением или несогласные с увольнением, они оставляют "черные ходы" для последующей возможности злонамеренного использования ресурсов, похищения конфиденциальной информации и т. д.

Промышленный шпионаж

Это самая сложная категория. Если ваши данные интересны кому-либо, то этот кто-то найдет способы достать их. Взлом хорошо защищенной сети - не самый простой вариант. Очень может статься, что уборщица "тетя Глаша", моющая под столом и ругающаяся на непонятный ящик с проводами, может оказаться хакером весьма высокого класса.

Халатность

Самая обширная категория злоупотреблений: начиная с не установленных вовремя обновлений, неизмененных настроек "по умолчанию" и заканчивая несанкционированными модемами для выхода в Internet, - в результате чего злоумышленники получают открытый доступ в хорошо защищенную сеть.

Низкая квалификация

Часто низкая квалификация не позволяет пользователю понять, с чем он имеет дело; из-за этого даже хорошие программы защиты становятся настоящей морокой системного администратора, и он вынужден надеяться только на защиту периметра. Большинство пользователей не понимают реальной угрозы от запуска исполняемых файлов и скриптов и считают, что исполняемые файлы -только файлы с расширением "exe". Низкая квалификация не позволяет также определить, какая информация является действительно конфиденциальной, а какую можно разглашать. В крупных компаниях часто можно позвонить пользователю и, представившись администратором, узнать у него учетные

данные для входа в сеть. Выход только один -обучение пользователей, создание соответствующих документов и повышение квалификации.

Методы защиты

Согласно статистике потерь, которые несут организации от различных компьютерных преступлений, львиную долю занимают потери от преступлений, совершаемых собственными нечистоплотными сотрудниками. Однако в последнее время наблюдается явная тенденция к увеличению потерь от внешних злоумышленников. В любом случае необходимо обеспечить защиту как от нелояльного персонала, так и от способных проникнуть в вашу сеть хакеров. Только комплексный подход к защите информации может внушить уверенность в ее безопасности.

Однако в связи с ограниченным объемом данной статьи рассмотрим только основные из технических методов защиты сетей и циркулирующей по ним информации, а именно - криптографические алгоритмы и их применение в данной сфере.

Защита данных от внутренних угроз

Для защиты циркулирующей в локальной сети информации можно применить следующие криптографические методы:

- шифрование информации;
- электронную цифровую подпись (ЭЦП).
- Шифрование

Шифрование информации помогает защитить ее конфиденциальность, т.е. обеспечивает невозможность несанкционированного ознакомления с ней. Шифрование - это процесс преобразования открытой информации в закрытую, зашифрованную (что называется "зашифрование") и наоборот ("расшифрование"). Это преобразование выполняется по строгим математическим алгоритмам; помимо собственно данных в преобразовании также участвует дополнительный элемент - "ключ". В ГОСТ 28147-89 дается следующее определение ключа: "Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований". Иными словами, ключ представляет собой уникальный элемент, позволяющий зашифровать информацию так, что получить открытую информацию из зашифрованной можно только определенному пользователю или группе пользователей.

Шифрование можно выразить следующими формулами:

$C=Ek_1(M)$ - зашифрование,

$M'=Dk_2(C)$ - расшифрование.

Функция E выполняет зашифрование информации, функция D – расшифрование. В том случае, если ключ k_2 соответствует ключу k_1, примененному при зашифровании, удается получить открытую информацию, т.е. получить соответствие $M' = M$.

При отсутствии же правильного ключа k_2 получить исходное сообщение практически невозможно.

По виду соответствия ключей k_1 и k_2 алгоритмы шифрования разделяются на две категории:

1) Симметричное шифрование: $k_1 = k_2$. Для зашифрования и расшифрования информации используется один и тот же ключ. Это означает, что пользователи, обменивающиеся зашифрованной информацией, должны иметь один и тот же ключ. Более безопасный вариант - существует уникальный ключ шифрования для каждой пары пользователей, который неизвестен остальным. Ключ симметричного шифрования должен храниться в секрете: его компрометация (утеря или хищение) повлечет за собой раскрытие всей зашифрованной данным ключом информации.

2) Асимметричное шифрование. Ключ k_1- в данном случае называется "открытым", а ключ k_2 - "секретным". Открытый ключ вычисляется из секретного различными способами (зависит от конкретного алгоритма шифрования). Обратное же вычисление k_2 из k_1 является практически невозможным. Смысл асимметричного шифрования состоит в том, что ключ k_2 хранится в секрете у его владельца и не должен быть известен никому; ключ k1, наоборот, распространяется всем пользователям, желающим отправлять зашифрованные сообщения владельцу ключа k_2; любой из них может зашифровать информацию на ключе k_1, расшифровать же ее может только обладатель секретного ключа k_2.

Оба ключа: ключ симметричного и секретный ключ асимметричного шифрования должны быть абсолютно случайными - в противном случае злоумышленник теоретически имеет возможность спрогнозировать значение определенного ключа. Поэтому для генерации ключей обычно используют датчики случайных чисел (ДСЧ), лучше всего - аппаратные.

Стоит сказать, что все государственные организации РФ и ряд коммерческих обязаны для защиты данных использовать отечественный алгоритм симметричного шифрования ГОСТ 28147-89. Это сильный криптографический алгоритм, в котором пока еще не найдено недостатков за более чем 12 лет применения.

ЭЦП

ЭЦП позволяет гарантировать целостность и авторство информации. Как видно из схемы, ЭЦП также использует криптографические ключи: секретный и открытый. Открытый ключ вычисляется из секретного по достаточно легкой формуле, например: $y=a^x \bmod p$ (где x - секретный ключ, y - открытый ключ, а и p- параметры алгоритма ЭЦП), обратное же вычисление весьма трудоемко и считается неосуществимым за приемлемое время при современных вычислительных мощностях.

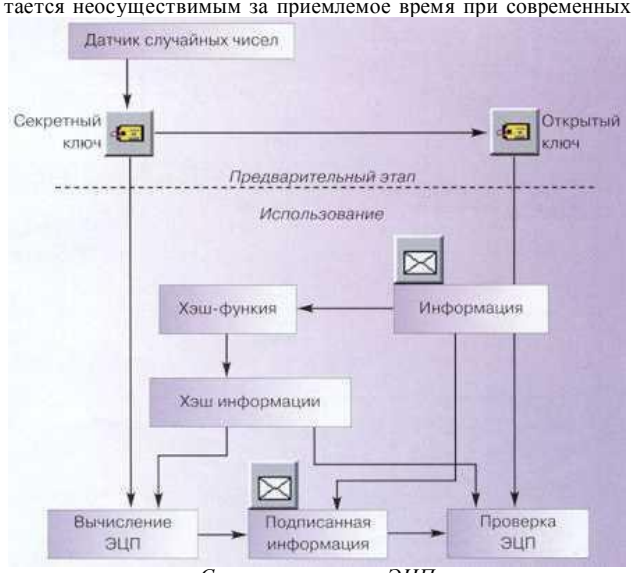


Схема применения ЭЦП

Схема распространения ключей ЭЦП аналогична схеме асимметричного шифрования: секретный ключ должен оставаться у его владельца, открытый же распространяется всем пользователям, желающим проверять ЭЦП владельца секретного ключа. Необходимо обеспечивать недоступность своего секретного ключа, ибо злоумышленник легко может подделать ЭЦП любого пользователя, получив доступ к его секретному ключу.

Электронной подписью можно подписать любую информацию. Предварительно информацию обрабатывают функцией хэширования, цель которой - выработка последовательности определенной длины, однозначно отражающей содержимое подписываемой информации. Данная последовательность называется "хэш", основное свойство хэша таково, что исключительно сложно модифицировать информацию так, чтобы ее хэш остался неизменным. Отечественный стандарт хэш-функций ГОСТ Р 34.11-94 предусматривает хэш размером 256 бит.

На основе хэша информации и секретного ключа пользователя вычисляется ЭЦП. Как правило, ЭЦП отправляется вместе с подписанной информацией (ЭЦП файла чаще всего просто помещают в конец файла перед его отправкой куда-либо по сети). Сама ЭЦП, как и хэш, является бинарной последовательностью фиксированного размера. Однако, помимо ЭЦП, к информации обычно добавляется также ряд служебных полей, прежде всего, идентификационная информация о пользователе, поставившем ЭЦП; причем, данные поля участвуют в расчете хэша. При проверке ЭЦП файла в интерактивном режиме результат может выглядеть так:

"Подпись файла "Document.doc" верна: Иванов А.А. 25.02.2003".

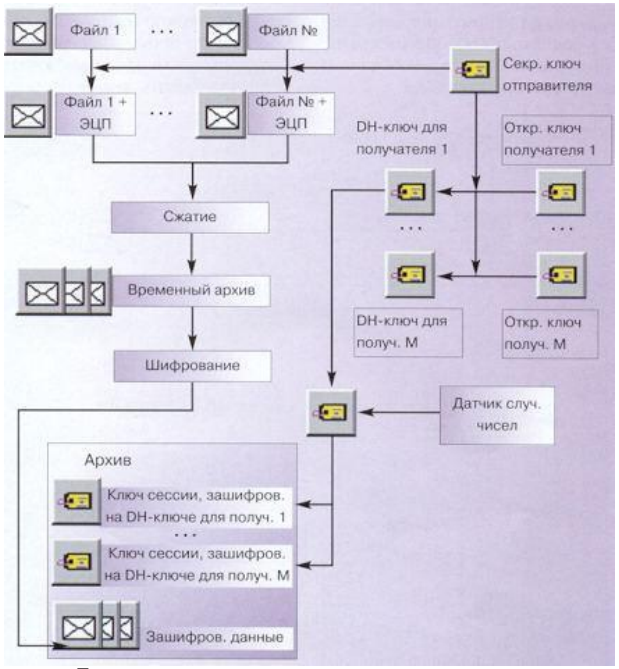
Естественно, в случае неверной ЭЦП выводится соответствующая информация, содержащая причину признания ЭЦП неверной. При проверке ЭЦП также вычисляется хэш информации; если он не совпадает с полученным при вычислении ЭЦП (что может означать попытку модификации информации злоумышленником), ЭЦП будет неверна.

Наряду с ГОСТ 28147-89 существует отечественный алгоритм ЭЦП: ГОСТ Р 34.10-94 и его более новый вариант ГОСТ Р 34.10-2001. Государственные организации РФ и ряд коммерческих обязаны использовать один из этих алгоритмов ЭЦП в паре с алгоритмом хэширования ГОСТ Р 34.11 - 94.

Существует и более простой способ обеспечения целостности информации - вычисление имитоприставки. Имитоприставка - это криптографическая контрольная сумма информации, вычисляемая с использованием ключа шифрования. Для вычисления имитоприставки используется, в частности, один из режимов работы алгоритма ГОСТ 28147-89, позволяющий получить в качестве имитоприставки 32-битную последовательность из информации любого размера. Аналогично хэшу информации имитоприставку чрезвычайно сложно подделать. Использование имитоприставок более удобно, чем применение ЭЦП: во-первых, 4 байта информации намного проще добавить, например, к пересылаемому по сети IP-пакету, чем большую структуру ЭЦП, во-вторых, вычисление имитоприставки существенно менее ресурсоемкая операция, чем формирование ЭЦП, поскольку в последнем случае используются такие сложные операции, как возведение 512-битного числа в степень, показателем которой является 256-битное число, что требует достаточно много вычислений. Имитоприставку нельзя использовать для контроля авторства сообщения, но этого во многих случаях и не требуется.

Комплексное применение криптографических алгоритмов

Для безопасной передачи по сети каких-либо файлов, их достаточно подписать и зашифровать. На схеме 3 представлена технология специализированного архивирования, обеспечивающая комплексную защиту файлов перед отправкой по сети.



Технология специализированного архивирования

Прежде всего, файлы подписываются секретным ключом отправителя, затем сжимаются для более быстрой передачи. Подписанные и сжатые файлы шифруются на случайном ключе сессии, который нужен только для зашифрования этой порции файлов -ключ берется с датчика случайных чисел, который обязан присутствовать в любом шифраторе. После этого к сформированному таким образом спецархиву добавляется заголовок, содержащий служебную информацию.

Заголовок позволяет расшифровать данные при получении. Для этого он содержит ключ сессии в зашифрованном виде. После зашифрования данных и записи их в архив, ключ сессии, в свою очередь, зашифровывается на ключе парной связи (DH-ключ), который вычисляется динамически из секретного ключа отправителя файлов и открытого ключа получателя по алгоритму Диффи-Хеллмана. Ключи парной связи различны для каждой пары "отправитель-получатель". Тот же самый ключ парной связи может быть вычислен только тем получателем, открытый ключ которого участвовал в вычислении ключа парной связи на стороне отправителя. Получатель для вычисления ключа парной связи использует свой секретный ключ и открытый ключ отправителя. Алгоритм Диффи-Хеллмана позволяет при этом получить тот же ключ, который сформировал отправитель из своего секретного ключа и открытого ключа получателя.

Таким образом, заголовок содержит копии ключа сессии (по количеству получателей), каждая их которых зашифрована на ключе парной связи отправителя для определенного получателя.

После получения архива получатель вычисляет ключ парной связи, затем расшифровывает ключ сессии, и наконец, расшифровывает собственно архив. После расшифрования информация автоматически разжимается. В последнюю очередь проверяется ЭЦП каждого файла.

Защита от внешних угроз

Методов защиты от внешних угроз придумано немало - найдено противодействие практически против всех опасностей, перечисленных в первой части данной статьи. Единственная проблема, которой пока не найдено адекватного решения, - DDoS-атаки. Рассмотрим технологию виртуальных частных сетей (VPN - Virtual Private Network), позволяющую с помощью криптографических методов как защитить информацию, передаваемую через Internet, так и пресечь несанкционированный доступ в локальную сеть снаружи.

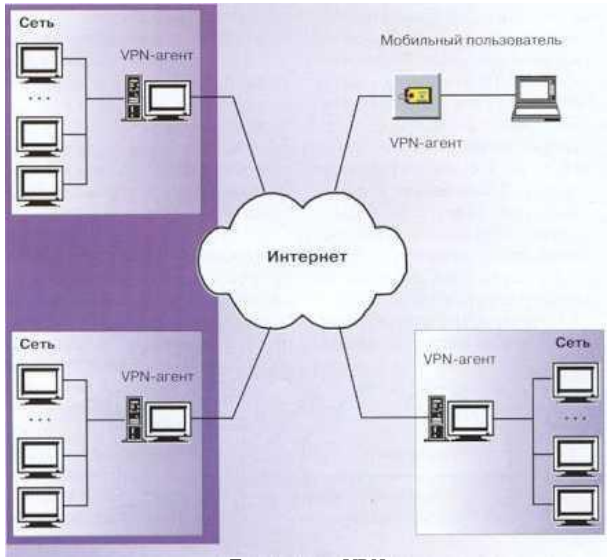
Виртуальные частные сети

На наш взгляд, технология VPN является весьма эффективной защитой, ее повсеместное внедрение - только вопрос времени. Доказательством этого является хотя бы внедрение поддержки VPN в последние операционные системы фирмы Microsoft - начиная с Windows 2000.

Суть VPN состоит в следующем (см. схему 4):

На все компьютеры, имеющие выход в Internet (вместо Internet может быть и любая другая сеть общего пользования), ставится средство, реализующее VPN. Такое средство обычно называют VPN-агентом. VPN-агенты обязательно должны быть установлены на все выходы в глобальную сеть.

VPN-агенты автоматически зашифровывают всю информацию, передаваемую через них в Internet, а также контролируют целостность информации с помощью имитовставок.



Технология VPN

Как известно, передаваемая в Internet информация представляет собой множество пакетов протокола IP, на которые она разбивается перед отправкой и может многократно переразбиваться по дороге. VPN-агенты обрабатывают именно IP-пакеты, ниже описана технология их работы.

1. Перед отправкой IP-пакета VPN-агент выполняет следующее:

Анализируется IP-адрес получателя пакета. В зависимости от адреса и другой информации (см. ниже) выбираются алгоритмы защиты данного пакета (VPN-агенты могут, поддерживать одновременно несколько алгоритмов шифрования и контроля целостности) и криптографические ключи. Пакет может и вовсе быть отброшен, если в настройках VPN-агента такой получатель не значится.

- Вычисляется и добавляется в пакет его имитовставка.
- Пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию).

Формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента. Это называется инкапсуляцией пакета. При использовании инкапсуляции обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для внешней атаки информация, например, внутренние IP-адреса сети, в этом случае недоступна.

2. При получении IP-пакета выполняются обратные действия:

Из заголовка пакета получается информация о VPN-агенте отправителя пакета. Если такой отправитель не входит в число разрешенных в настройках, то пакет отбрасывается. То же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком.

Согласно настройкам выбираются криптографические алгоритмы и ключи.

Пакет расшифровывается, затем проверяется его целостность. Пакеты с нарушенной целостностью также отбрасываются.

В завершение обработки пакет в его исходном виде отправляется настоящему адресату по локальной сети.

Все перечисленные операции выполняются автоматически, работа VPN-агентов является незаметной для пользователей. Сложной является только настройка VPN-агентов, которая может быть выполнена только очень опытным пользователем. VPN-агент может находиться непосредственно на защищаемом компьютере (что особенно полезно для мобильных пользователей). В этом случае он защищает обмен данными только одного компьютера - на котором установлен.

VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (к таким каналам обычно применяется термин "туннель", а технология их создания называется "туннелированием"). Вся информация идет по туннелю только в зашифрованном виде. Кстати, пользователи VPN при обращении к компьютерам из удаленных локальных сетей могут и не знать, что эти компьютеры реально находятся, может быть, в другом городе, - разница между удаленными и локальными компьютерами в данном случае состоит только в скорости передачи данных.

Как видно из описания действий VPN-агентов, часть IP-пакетов ими отбрасывается. Действительно, VPN-агенты фильтруют пакеты согласно своим настройкам (совокупность настроек VPN-агента называется "Политикой безопасности"). То есть VPN-агент выполняет два основных действия: создание туннелей и фильтрация пакетов (см.схему 5).

Туннелирование и фильтрация

IP-пакет отбрасывается или направляется в конкретный туннель в зависимости от значений следующих его характеристик:

- IP-адрес источника (для исходящего пакета - адрес конкретного компьютера защищаемой сети).
- IP-адрес назначения.

Протокол более верхнего уровня, которому принадлежит данный пакет (например, TCP или UDP для транспортного уровня).

Номер порта, с которого или на который отправлен пакет (например, 1080).

Более подробно технология VPN описана в специальной литературе.

Лекция 12. Обеспечение высокой доступности

Доступность

Основные понятия

Информационная система предоставляет своим пользователям определенный набор услуг (сервисов). Говорят, что обеспечен нужный уровень доступности этих сервисов, если следующие показатели находятся в заданных пределах:

Эффективность услуг. Эффективность услуги определяется в терминах максимального времени обслуживания запроса, количества поддерживаемых пользователей и т.п. Требуется, чтобы эффективность не опускалась ниже заранее установленного порога.

Время недоступности. Если эффективность информационной услуги не удовлетворяет наложенным ограничениям, услуга считается недоступной. Требуется, чтобы максимальная продолжительность периода недоступности и суммарное время недоступности за некоторой период (месяц, год) не превышали заранее заданных пределов.

В сущности, требуется, чтобы информационная система почти всегда работала с нужной эффективностью. Для некоторых критически важных систем (например, систем управления) время недоступности должно быть нулевым, без всяких "почти". В таком случае говорят о вероятности возникновения ситуации недоступности и требуют, чтобы эта вероятность не превышала заданной величины. Для решения данной задачи создавались и создаются специальные **отказоустойчивые системы**, стоимость которых, как правило, весьма высока.

К подавляющему большинству коммерческих систем предъявляются менее жесткие требования, однако современная деловая жизнь и здесь накладывает достаточно суровые ограничения, когда число обслуживаемых пользователей может измеряться тысячами, время ответа не должно превышать нескольких секунд, а время недоступности - нескольких часов в год.

Задачу обеспечения **высокой доступности** необходимо решать для современных конфигураций, построенных в технологии клиент/сервер. Это означает, что в защите нуждается вся цепочка - от пользователей (возможно, удаленных) до критически важных серверов (в том числе серверов безопасности).

Основные угрозы доступности были рассмотрены нами ранее.

В соответствии с ГОСТ 27.002, под **отказом** понимается событие, которое заключается в нарушении работоспособности изделия. В контексте данной работы изделие - это информационная система или ее компонент.

В простейшем случае можно считать, что отказы любого компонента составного изделия ведут к общему отказу, а распределение отказов во времени представляет собой простой **пуассоновский поток событий.** В таком случае вводят понятие **интенсивности отказов и** среднего времени наработки на отказ, которые связаны между собой соотношением

$$T_i = 1/l_i$$

где i - номер компонента,

l_i - интенсивность отказов,

T_i - среднее время наработки на отказ.

Интенсивности отказов независимых компонентов складываются:

$$l = l_1 + \ldots + l_n$$

а среднее время наработки на отказ для составного изделия задается соотношением

$$T = 1/l$$

Уже эти простейшие выкладки показывают, что если существует компонент, интенсивность отказов которого много больше, чем у остальных, то именно он определяет среднее время наработки на отказ всей информационной системы. Это является теоретическим обоснованием принципа первоочередного укрепления самого слабого звена.

Пуассоновская модель позволяет обосновать еще одно очень важное положение, состоящее в том, что эмпирический подход к построению систем высокой доступности не может быть реализован за приемлемое время. При традиционном цикле тестирования/отладки программной системы по оптимистическим оценкам каждое исправление ошибки приводит к экспоненциальному убыванию (примерно на половину десятичного порядка) интенсивности отказов. Отсюда следует, что для того, чтобы на опыте убедиться в достижении необходимого уровня доступности, независимо от применяемой технологии тестирования и отладки, придется потратить время, практически равное среднему времени наработки на отказ. Например, для достижения среднего времени наработки на отказ 105 часов потребуется более 104,5 часов, что составляет более трех лет. Значит, нужны иные методы построения систем высокой доступности, методы, эффективность которых доказана аналитически или практически за более чем пятьдесят лет развития вычислительной техники и программирования.

Пуассоновская модель применима в тех случаях, когда информационная система содержит одиночные точки отказа, то есть компоненты, выход которых из строя ведет к отказу всей системы. Для исследования систем с резервированием применяется иной формализм.

В соответствии с постановкой задачи будем считать, что существует количественная мера эффективности предоставляемых изделием информационных услуг. В таком случае вводятся понятия показателей эффективности отдельных элементов и эффективности функционирования всей сложной системы.

В качестве меры доступности можно принять вероятность приемлемости эффективности услуг, предоставляемых информационной системой, на всем протяжении рассматриваемого отрезка времени. Чем большим запасом эффективности располагает система, тем выше ее доступность.

При наличии избыточности в конфигурации системы вероятность того, что в рассматриваемый промежуток времени эффективность информационных сервисов не опустится ниже допустимого предела, зависит не только от вероятности отказа компонентов, но и от времени, в течение которого они остаются неработоспособными, поскольку при этом суммарная эффективность падает, и каждый следующий отказ может стать фатальным. Чтобы максимально увеличить доступность системы, необходимо минимизировать время неработоспособности каждого компонента. Кроме того, следует учитывать, что, вообще говоря, ремонтные работы могут потребовать понижения эффективности или даже временного отключения работоспособных компонентов; такого рода влияние также необходимо минимизировать.

Несколько терминологических замечаний. Обычно в литературе по теории надежности вместо доступности говорят о готовности (в том числе о высокой готовности). Мы предпочли термин "доступность", чтобы подчеркнуть, что информационный сервис должен быть не просто "готов" сам по себе, но доступен для своих пользователей в условиях, когда ситуации недоступности могут вызываться причинами, на первый взгляд не имеющими прямого отношения к сервису (пример - отсутствие консультационного обслуживания).

Далее, вместо времени недоступности обычно говорят о коэффициенте готовности. Нам хотелось обратить внимание на два показателя - длительность однократного простоя и суммарную продолжительность простоев, поэтому мы предпочли термин "время недоступности" как более емкий.

Основы мер обеспечения высокой доступности

Основой мер повышения доступности является применение структурированного подхода, нашедшего воплощение в объектно-ориентированной методологии. **Структуризация** необходима по отношению ко всем аспектам и составным частям информационной системы - от архитектуры до административных баз данных, на всех этапах ее жизненного цикла - от инициации до выведения из эксплуатации. Структуризация, важная сама по себе, является одновременно необходимым условием практической реализуемости прочих мер повышения доступности. Только маленькие системы можно строить и эксплуатировать как угодно. У больших систем свои законы, которые, как мы уже указывали, программисты впервые осознали более 30 лет назад.

При разработке мер обеспечения высокой доступности информационных сервисов рекомендуется руководствоваться следующими архитектурными принципами, рассматривавшимися ранее:

- апробированность всех процессов и составных частей информационной системы;
- унификация процессов и составных частей;
- управляемость процессов, контроль состояния частей;
- автоматизация процессов;
- модульность архитектуры;
- ориентация на простоту решений.

Доступность системы в общем случае достигается за счет применения трех групп мер, направленных на повышение:

- безотказности (под этим понимается минимизация вероятности возникновения какого-либо отказа; это элемент пассивной безопасности, который дальше рассматриваться не будет);
- отказоустойчивости (способности к нейтрализации отказов, "живучести", то есть способности сохранять требуемую эффективность, несмотря на отказы отдельных компонентов);
- обслуживаемости (под обслуживаемостью понимается минимизация времени простоя отказавших компонентов, а также отрицательного влияния ремонтных работ на эффектив-

ность информационных сервисов, то есть быстрое и безопасное восстановление после отказов).

Главное при разработке и реализации мер обеспечения высокой доступности - **полнота** и **систематичность**. В этой связи представляется целесообразным составить (и поддерживать в актуальном состоянии) **карту информационной системы** организации (на что мы уже обращали внимание), в которой фигурировали бы все объекты ИС, их состояние, связи между ними, процессы, ассоциируемые с объектами и связями. С помощью подобной карты удобно формулировать намечаемые меры, контролировать их исполнение, анализировать состояние ИС.

Отказоустойчивость и зона риска

Информационную систему можно представить в виде графа сервисов, ребра в котором соответствуют отношению "сервис А непосредственно использует сервис В".

Пусть в результате осуществления некоторой атаки (источником которой может быть как человек, так и явление природы) выводится из строя подмножество сервисов S1 (то есть эти сервисы в результате нанесенных повреждений становятся неработоспособными). Назовем S1 зоной поражения.

В зону риска S мы будем включать все сервисы, эффективность которых при осуществлении атаки падает ниже допустимого предела. Очевидно, S1 - подмножество S. S строго включает S1, когда имеются сервисы, непосредственно не затронутые атакой, но критически зависящие от пораженных, то есть неспособные переключиться на использование эквивалентных услуг либо в силу отсутствия таковых, либо в силу невозможности доступа к ним. Например, зона поражения может сводиться к одному порту концентратора, обслуживающему критичный сервер, а зона риска охватывает все рабочие места пользователей сервера.

Чтобы система не содержала одиночных точек отказа, то есть оставалась "живучей" при реализации любой из рассматриваемых угроз, ни одна зона риска не должна включать в себя предоставляемые услуги. Нейтрализацию отказов нужно выполнять внутри системы, незаметно для пользователей, за счет размещения достаточного количества избыточных ресурсов.

С другой стороны, естественно соизмерять усилия по обеспечению "живучести" с рассматриваемыми угрозами. Когда рассматривается набор угроз, соответствующие им зоны поражения могут оказаться вложенными, так что "живучесть" по отношению к более серьезной угрозе автоматически влечет за собой и "живучесть" в более легких случаях. Следует учитывать, однако, что обычно стоимость переключения на резервные ресурсы растет вместе с увеличением объема этих ресурсов. Значит, для наиболее вероятных угроз целесообразно минимизировать зону риска, даже если предусмотрена нейтрализация объемлющей угрозы. Нет смысла переключаться на резервный вычислительный центр только потому, что у одного из серверов вышел из строя блок питания.

Зону риска можно трактовать не только как совокупность ресурсов, но и как часть пространства, затрагиваемую при реализации угрозы. В таком случае, как правило, чем больше расстояние дублирующего ресурса от границ зоны риска, тем выше стоимость его поддержания, поскольку увеличивается протяженность линий связи, время переброски персонала и т.п. Это еще один довод в пользу адекватного противодействия угрозам, который следует принимать во внимание при размещении избыточных ресурсов и, в частности, при организации резервных центров.

Введем еще одно понятие. Назовем зоной нейтрализации угрозы совокупность ресурсов, вовлеченных в нейтрализацию отказа, возникшего вследствие реализации угрозы. Имеются в виду ресурсы, режим работы которых в случае отказа изменяется. Очевидно, зона риска является подмножеством зоны нейтрализации. Чем меньше разность между ними, тем экономичнее данный механизм нейтрализации.

Все, что находится вне зоны нейтрализации, отказа "не чувствует" и может трактовать внутренность этой зоны как безотказную. Таким образом, в иерархически организованной системе грань между "живучестью" и обслуживаемостью, с одной стороны, и безотказностью, с другой стороны, относительна. Целесообразно конструировать целостную информационную систему из компонентов, которые на верхнем уровне можно считать безотказными, а вопросы "живучести" и обслуживаемости решать в пределах каждого компонента.

Обеспечение отказоустойчивости

Основным средством повышения "живучести" является внесение избыточности в конфигурацию аппаратных и программных средств, поддерживающей инфраструктуры и персонала, резервирование технических средств и тиражирование информационных ресурсов (программ и данных).

Меры по обеспечению отказоустойчивости можно разделить на локальные и распределенные. Локальные меры направлены на достижение "живучести" отдельных компьютерных систем или их аппаратных и программных компонентов (в первую очередь с целью нейтрализации внутренних отказов ИС). Типичные примеры подобных мер - использование кластерных конфигураций в качестве платформы критичных серверов или "горячее" резервирование активного сетевого оборудования с автоматическим переключением на резерв.

Если в число рассматриваемых рисков входят серьезные аварии поддерживающей инфраструктуры, приводящие к выходу из строя производственной площадки организации, следует предусмотреть распределенные меры обеспечения живучести, такие как создание или аренда резервного вычислительного центра. При этом, помимо дублирования и/или тиражирования ресурсов, необходимо предусмотреть средства автоматического или быстрого ручного переконфигурирования компонентов ИС, чтобы обеспечить переключение с основной площадки на резервную.

Аппаратура - относительно статичная составляющая, однако было бы ошибкой полностью отказывать ей в динамичности. В большинстве организаций информационные системы находятся в постоянном развитии, поэтому на протяжении всего жизненного цикла ИС следует соотносить все изменения с необходимостью обеспечения "живучести", не забывать "тиражировать" новые и модифицированные компоненты.

Программы и данные более динамичны, чем аппаратура, и резервироваться они могут постоянно, при каждом изменении, после завершения некоторой логически замкнутой группы изменений или по истечении определенного времени.

Резервирование программ и данных может выполняться многими способами - за счет зеркалирования дисков, резервного копирования и восстановления, репликации баз данных и т.п. Будем использовать для всех перечисленных способов термин "тиражирование".

Выделим следующие классы тиражирования:

- **Симметричное/асимметричное**. Тиражирование называется симметричным, если все серверы, предоставляющие данный сервис, могут изменять принадлежащую им информацию и передавать изменения другим серверам. В противном случае тиражирование называется асимметричным.
- **Синхронное/асинхронное.** Тиражирование называется синхронным, если изменение передается всем экземплярам сервиса в рамках одной распределенной транзакции. В противном случае тиражирование называется асинхронным.
- Осуществляемое средствами сервиса, хранящего информацию/внешними средствами.

Рассмотрим, какие способы тиражирования предпочтительнее.

Безусловно, следует предпочесть стандартные средства тиражирования, встроенные в сервис.

Асимметричное тиражирование теоретически проще симметричного, поэтому целесообразно выбрать асимметрию.

Труднее всего выбрать между синхронным и асинхронным тиражированием. Синхронное идейно проще, но его реализация может быть тяжеловесной и сложной, хотя это внутренняя сложность сервиса, невидимая для приложений. Асинхронное тиражирование устойчивее к отказам в сети, оно меньше влияет на работу основного сервиса.

Чем надежнее связь между серверами, вовлеченными в процесс тиражирования, чем меньше время, отводимое на переключение с основного сервера на резервный, чем жестче требования к актуальности информации, тем более предпочтительным оказывается синхронное тиражирование.

С другой стороны, недостатки асинхронного тиражирования могут компенсироваться процедурными и программными мерами, направленными на контроль целостности информации в распределенной ИС. Сервисы, входящие в состав ИС, в состоянии обеспечить ведение и хранение журналов транзакций, с помощью которых можно выявлять операции, утерянные при переключении на резервный сервер. Даже в условиях неустойчивой связи с удаленными филиалами организации подобная проверка в фоновом режиме займет не более нескольких часов, поэтому асинхронное тиражирование может использоваться практически в любой ИС.

Асинхронное тиражирование может производиться на сервер, работающий в режиме "горячего" резерва, возможно, даже обслуживающего часть пользовательских запросов, или на сервер, работающий в режиме "теплого" резерва, когда изменения периодически "накатываются", но сам резервный сервер запросов не обслуживает.

Достоинство "теплого" резервирования в том, что его можно реализовать, оказывая меньшее влияние на основной сервер. Это влияние вообще может быть сведено к нулю, если асинхронное тиражирование осуществляется путем передачи инкрементальных копий с основного сервера (резервное копирование необходимо выполнять в любом случае).

Основной недостаток "теплого" резерва состоит в длительном времени включения, что может быть неприемлемо для "тяжелых" серверов, таких как кластерная конфигурация сервера СУБД. Здесь необходимо проводить измерения в условиях, близких к реальным.

Второй недостаток "теплого" резерва вытекает из опасности малых изменений. Может оказаться, что в самый нужный момент срочный перевод резерва в штатный режим невозможен.

Учитывая приведенные соображения, следует в первую очередь рассматривать возможность "горячего" резервирования, либо тщательно контролировать использование "теплого" резерва и регулярно (не реже одного раза в неделю) проводить пробные переключения резерва в "горячий" режим.

Программное обеспечение промежуточного слоя

С помощью программного обеспечения промежуточного слоя (ПО ПС) можно для произвольных прикладных сервисов добиться высокой "живучести" с полностью прозрачным для пользователей переключением на резервные мощности.

О возможностях и свойствах ПО промежуточного слоя можно прочитать в статье Ф. Бернстайна "Middleware: модель сервисов распределенной системы" (Jet Info, 1997, 11).

Перечислим основные достоинства ПО ПС, существенные для обеспечения высокой доступности.

- ПО ПС уменьшает сложность создания распределенных систем. Подобное ПО берет на себя часть функций, которые в локальном случае выполняют операционные системы;
- ПО ПС берет на себя маршрутизацию запросов, позволяя тем самым обеспечить "живучесть" прозрачным для пользователей образом;
- ПО ПС осуществляет балансировку загрузки вычислительных мощностей, что также способствует повышению доступности данных;
- ПО ПС в состоянии осуществлять тиражирование любой информации, а не только содержимого баз данных. Следовательно, любое приложение можно сделать устойчивым к отказам серверов;
- ПО ПС в состоянии отслеживать состояние приложений и при необходимости тиражировать и перезапускать программы, что гарантирует "живучесть" программных систем;
- ПО ПС дает возможность прозрачным для пользователей образом выполнять переконфигурирование (и, в частности, наращивание) серверных компонентов, что позволяет масштабировать систему, сохраняя инвестиции в прикладные системы. Стабильность прикладных систем - важный фактор повышения доступности данных.

Ранее мы упоминали о достоинствах использования ПО ПС в рамках межсетевых экранов, которые в таком случае становятся элементом обеспечения отказоустойчивости предоставляемых информационных сервисов.

Обеспечение обслуживаемости

Меры по обеспечению обслуживаемости направлены на снижение сроков диагностирования и устранения отказов и их последствий.

Для обеспечения обслуживаемости рекомендуется соблюдать следующие архитектурные принципы:

- ориентация на построение информационной системы из унифицированных компонентов с целью упрощения замены отказавших частей;
- ориентация на решения модульной структуры с возможностью автоматического обнаружения отказов, динамического переконфигурирования аппаратных и программных средств и замены отказавших компонентов в "горячем" режиме.

Динамическое переконфигурирование преследует две основные цели:

- изоляция отказавших компонентов;
- сохранение работоспособности сервисов.

Изолированные компоненты образуют зону поражения реализованной угрозы. Чем меньше соответствующая зона риска, тем выше обслуживаемость сервисов. Так, при отказах блоков питания, вентиляторов и/или дисков в современных серверах зона риска ограничивается отказавшим компонентом; при отказах процессорных модулей весь сервер может потребовать перезагрузки (что способно вызвать дальнейшее расширение зоны риска). Очевидно, в идеальном случае зоны поражения и риска совпадают, и современные серверы и активное сетевое оборудование, а также программное обеспечение ведущих производителей весьма близки к этому идеалу.

Возможность программирования реакции на отказ также повышает обслуживаемость систем. Каждая организация может выбрать свою стратегию реагирования на отказы тех или иных аппаратных и программных компонентов и автоматизировать эту реакцию. Так, в простейшем случае возможна отправка сообщения системному администратору, чтобы ускорить начало ремонтных работ; в более сложном случае может быть реализована процедура "мягкого" выключения (переключения) сервиса, чтобы упростить обслуживание.

Возможность удаленного выполнения административных действий - важное направление повышения обслуживаемости, поскольку при этом ускоряется начало восстановительных мероприятий, а в идеале все работы (обычно связанные с обслуживанием программных компонентов) выполняются в удаленном режиме, без перемещения квалифицированного персонала, то есть с высоким качеством и в кратчайшие сроки. Для современных систем возможность удаленного администрирования - стандартное свойство, но важно позаботиться о его практической реализуемости в условиях разнородности конфигураций (в первую очередь клиентских). Централизованное распространение и конфигурирование программного обеспечения, управление компонентами информационной системы и диагностирование - надежный фундамент технических мер повышения обслуживаемости.

Существенный аспект повышения обслуживаемости - организация консультационной службы для пользователей (обслуживаемость пользователей), внедрение программных систем для работы этой службы, обеспечение достаточной пропускной способности каналов связи с пользователями, в том числе в режиме пиковых нагрузок.

Лекция 13. Туннелирование и управление

Туннелирование

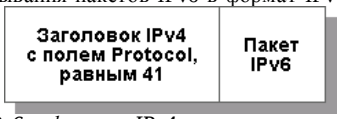
На наш взгляд, **туннелирование** следует рассматривать как самостоятельный сервис безопасности. Его суть состоит в том, чтобы "упаковать" передаваемую порцию данных, вместе со служебными полями, в новый "конверт". В качестве синонимов термина "туннелирование" могут использоваться **"конвертование"** и **"обертывание"**.

Туннелирование может применяться для нескольких целей:

- передачи через сеть пакетов, принадлежащих протоколу, который в данной сети не поддерживается (например, передача пакетов IPv6 через старые сети, поддерживающие только IPv4);
- обеспечения слабой формы конфиденциальности (в первую очередь конфиденциальности трафика) за счет сокрытия истинных адресов и другой служебной информации;
- обеспечения конфиденциальности и целостности передаваемых данных при использовании вместе с криптографическими сервисами.

Туннелирование может применяться как на сетевом, так и на прикладном уровнях. Например, стандартизовано туннелирование для IP и двойное конвертование для почты X.400.

На рис. показан пример обертывания пакетов IPv6 в формат IPv4.



Обертывание пакетов IPv6 в формат IPv4 с целью их туннелирования через сети IPv4.

Комбинация туннелирования и шифрования (наряду с необходимой криптографической инфраструктурой) на выделенных шлюзах и экранирования на маршрутизаторах поставщиков сетевых услуг (для разделения пространств "своих" и "чужих" сетевых адресов в духе виртуальных локальных сетей) позволяет реализовать такое важное в современных условиях защитное средство, как **виртуальные частные сети**. Подобные сети, наложенные обычно поверх Internet, существенно дешевле и гораздо безопаснее, чем собственные сети организации, построенные на выделенных каналах. Коммуникации на всем их протяжении физически защитить невозможно, поэтому лучше изначально исходить из предположения об их уязвимости и соответственно обеспечивать защиту. Современные протоколы, направленные на поддержку классов обслуживания, помогут гарантировать для виртуальных частных сетей заданную пропускную способность, величину задержек и т.п., ликвидируя тем самым единственное на сегодня реальное преимущество сетей собственных.

Межсетевые экраны как точки реализации сервиса виртуальных частных сетей.

Концами туннелей, реализующих виртуальные частные сети, целесообразно сделать межсетевые экраны, обслуживающие подключение организаций к внешним сетям. В таком случае туннелирование и шифрование станут дополнительными преобразованиями, выполняемыми в процессе фильтрации сетевого трафика наряду с трансляцией адресов.

Концами туннелей, помимо корпоративных межсетевых экранов, могут быть мобильные компьютеры сотрудников (точнее, их персональные МЭ).

Управление

Основные понятия

Управление можно отнести к числу инфраструктурных сервисов, обеспечивающих нормальную работу компонентов и средств безопасности. Сложность современных систем такова, что без правильно организованного управления они постепенно деградируют как в плане эффективности, так и в плане защищенности.

Возможен и другой взгляд на управление - как на интегрирующую оболочку информационных сервисов и сервисов безопасности (в том числе средств обеспечения высокой доступности), обеспечивающую их нормальное, согласованное функционирование под контролем администратора ИС.

Согласно стандарту X.700, управление подразделяется на:

- мониторинг компонентов;
- контроль (то есть выдачу и реализацию управляющих воздействий);

- координацию работы компонентов системы.
- Системы управления должны:
- позволять администраторам планировать, организовывать, контролировать и учитывать использование информационных сервисов;
- давать возможность отвечать на изменение требований;
- обеспечивать предсказуемое поведение информационных сервисов;
- обеспечивать защиту информации.

Иными словами, управление должно обладать достаточно богатой функциональностью, быть результативным, гибким и информационно безопасным.

В X.700 выделяется пять функциональных областей управления:

- управление конфигурацией (установка параметров для нормального функционирования, запуск и остановка компонентов, сбор информации о текущем состоянии системы, прием извещений о существенных изменениях в условиях функционирования, изменение конфигурации системы);
- управление отказами (выявление отказов, их изоляция и восстановление работоспособности системы);
- управление производительностью (сбор и анализ статистической информации, определение производительности системы в штатных и нештатных условиях, изменение режима работы системы);
- управление безопасностью (реализация политики безопасности путем создания, удаления и изменения сервисов и механизмов безопасности, распространения соответствующей информации и реагирования на инциденты);
- управление учетной информацией (т.е. взимание платы за пользование ресурсами).

В стандартах семейства X.700 описывается модель управления, способная обеспечить достижение поставленных целей. Вводится понятие управляемого объекта как совокупности характеристик компонента системы, важных с точки зрения управления. К таким характеристикам относятся:

- атрибуты объекта;
- допустимые операции;
- извещения, которые объект может генерировать;
- связи с другими управляемыми объектами.

Согласно рекомендациям X.701, системы управления распределенными ИС строятся в архитектуре менеджер/агент. Агент (как программная модель управляемого объекта) выполняет управляющие действия и порождает (при возникновении определенных событий) извещения от его имени. В свою очередь, менеджер выдает агентам команды на управляющие воздействия и получает извещения.

Иерархия взаимодействующих менеджеров и агентов может иметь несколько уровней. При этом элементы промежуточных уровней играют двоякую роль: по отношению к вышестоящим элементам они являются агентами, а к нижестоящим - менеджерами. Многоуровневая архитектура менеджер/агент - ключ к распределенному, масштабируемому управлению большими системами.

Логически связанной с многоуровневой архитектурой является концепция доверенного (или делегированного) управления. При доверенном управлении менеджер промежуточного уровня может управлять объектами, использующими собственные протоколы, в то время как "наверху" опираются исключительно на стандартные средства.

Обязательным элементом при любом числе архитектурных уровней является управляющая консоль.

С точки зрения изучения возможностей систем управления следует учитывать разделение, введенное в X.701. Управление подразделяется на следующие аспекты:

- информационный (атрибуты, операции и извещения управляемых объектов);
- функциональный (управляющие действия и необходимая для них информация);
- коммуникационный (обмен управляющей информацией);
- организационный (разбиение на области управления).

Ключевую роль играет модель управляющей информации. Она описывается рекомендациями X.720. Модель является объектно-ориентированной с поддержкой инкапсуляции и наследования. Дополнительно вводится понятие пакета как совокупности атрибутов, операций, извещений и соответствующего поведения.

Класс объектов определяется позицией в дереве наследования, набором включенных пакетов и внешним интерфейсом, то есть видимыми снаружи атрибутами, операциями, извещениями и демонстрируемым поведением.

К числу концептуально важных можно отнести понятие "проактивного", то есть упреждающего управления. Упреждающее управление основано на предсказании поведения системы на основе текущих данных и ранее накопленной информации. Простейший пример подобного управления - выдача сигнала о возможных проблемах с диском после серии программно-нейтрализуемых ошибок чтения/записи. В более сложном случае определенный характер рабочей нагрузки и действий пользователей может предшествовать резкому замедлению работы системы; адекватным управляющим

воздействием могло бы стать понижение приоритетов некоторых заданий и извещение администратора о приближении кризиса.

Возможности типичных систем

Развитые системы управления имеют, если можно так выразиться, двухмерную настраиваемость - на нужды конкретных организаций и на изменения в информационных технологиях. Системы управления живут (по крайней мере, должны жить) долго. За это время в различных предметных областях администрирования (например, в области резервного копирования) наверняка появятся решения, превосходящие изначально заложенные в управляющий комплект. Последний должен уметь эволюционировать, причем разные его компоненты могут делать это с разной скоростью. Никакая жесткая, монолитная система такого не выдержит.

Единственный выход - наличие каркаса, с которого можно снимать старое и "навешивать" новое, не теряя эффективности управления.

Каркас как самостоятельный продукт необходим для достижения по крайней мере следующих целей:

- сглаживание разнородности управляемых информационных систем, предоставление унифицированных программных интерфейсов для быстрой разработки управляющих приложений;
- создание инфраструктуры управления, обеспечивающей наличие таких свойств, как поддержка распределенных конфигураций, масштабируемость, информационная безопасность и т.д.;
- предоставление функционально полезных универсальных сервисов, таких как планирование заданий, генерация отчетов и т.п.

Вопрос о том, что, помимо каркаса, должно входить в систему управления, является достаточно сложным Во-первых, многие системы управления имеют мэйнфреймовое прошлое и попросту унаследовали некоторую функциональность, которая перестала быть необходимой. Во-вторых, для ряда функциональных задач появились отдельные, высококачественные решения, превосходящие аналогичные по назначению "штатные" компоненты. Видимо, с развитием объектного подхода, многоплатформенности важнейших сервисов и их взаимной совместимости, системы управления действительно превратятся в каркас. Пока же на их долю остается достаточно важных областей, а именно:

- управление безопасностью;
- управление загрузкой;
- управление событиями;
- управление хранением данных;
- управление проблемными ситуациями;
- генерация отчетов.

На уровне инфраструктуры присутствует решение еще одной важнейшей функциональной задачи - обеспечение автоматического обнаружения управляемых объектов, выявление их характеристик и связей между ними.

Отметим, что управление безопасностью в совокупности с соответствующим программным интерфейсом позволяет реализовать платформно-независимое разграничение доступа к объектам произвольной природы и (что очень важно) вынести функции безопасности из прикладных систем. Чтобы выяснить, разрешен ли доступ текущей политикой, приложению достаточно обратиться к менеджеру безопасности системы управления.

Менеджер безопасности осуществляет идентификацию/аутентификацию пользователей, контроль доступа к ресурсам и протоколирование неудачных попыток доступа. Можно считать, что менеджер безопасности встраивается в ядро операционных систем контролируемых элементов ИС, перехватывает соответствующие обращения и осуществляет свои проверки перед проверками, выполняемыми ОС, так что он создает еще один защитный рубеж, не отменяя, а дополняя защиту, реализуемую средствами ОС.

Развитые системы управления располагают централизованной базой, в которой хранится информация о контролируемой ИС и, в частности, некоторое представление о политике безопасности. Можно считать, что при каждой попытке доступа выполняется просмотр сохраненных в базе правил, в результате которого выясняется наличие у пользователя необходимых прав. Тем самым для проведения единой политики безопасности в рамках корпоративной информационной системы закладывается прочный технологический фундамент.

Хранение параметров безопасности в базе данных дает администраторам еще одно важное преимущество - возможность выполнения разнообразных запросов. Можно получить список ресурсов, доступных данному пользователю, список пользователей, имеющих доступ к данному ресурсу и т.п.

Одним из элементов обеспечения высокой доступности данных является подсистема автоматического управления хранением данных, выполняющая резервное копирование данных, а также автоматическое отслеживание их перемещения между основными и резервными носителями.

Для обеспечения высокой доступности информационных сервисов используется управление загрузкой, которое можно подразделить на управление прохождением заданий и контроль производительности.

Контроль производительности - понятие многогранное. Сюда входят и оценка быстродействия компьютеров, и анализ пропускной способности сетей, и отслеживание числа одновременно поддерживаемых пользователей, и время реакции, и накопление и анализ статистики использования ресурсов. Обычно в распределенной системе соответствующие данные доступны "в принципе", они поставляются точечными средствами управления, но проблема получения целостной картины, как текущей, так и перспективной, остается весьма сложной. Решить ее способна только система управления корпоративного уровня.

Средства контроля производительности целесообразно разбить на две категории:

- выявление случаев неадекватного функционирования компонентов информационной системы и автоматическое реагирование на эти события;
- анализ тенденций изменения производительности системы и долгосрочное планирование.

Для функционирования обеих категорий средств необходимо выбрать отслеживаемые параметры и допустимые границы для них, выход за которые означает "неадекватность функционирования". После этого задача сводится к выявлению нетипичного поведения компонентов ИС, для чего могут применяться статистические методы.

Управление событиями (точнее, сообщениями о событиях) - это базовый механизм, позволяющий контролировать состояние информационных систем в реальном времени. Системы управления позволяют классифицировать события и назначать для некоторых из них специальные процедуры обработки. Тем самым реализуется важный принцип автоматического реагирования.

Очевидно, что задачи контроля производительности и управления событиями, равно как и методы их решения в системах управления, близки к аналогичным аспектам систем активного аудита. Налицо еще одно свидетельство концептуального единства области знаний под названием "информационная безопасность" и необходимости реализации этого единства на практике.

Лекция 14. Заключение

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

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

- доступность;
- целостность;
- конфиденциальность.

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

Важность проблематики ИБ объясняется двумя основными причинами:

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

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

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

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

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

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

- законодательного;
- административного;
- процедурного;

- программно-технического.

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

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

Законодательный, административный и процедурный уровни

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Необходимо всячески подчеркивать важность проблемы ИБ; сконцентрировать ресурсы на важнейших направлениях исследований; скоординировать образовательную деятельность; создать и поддерживать негативное отношение к нарушителям ИБ - все это функции законодательного уровня.

На законодательном уровне особого внимания заслуживают правовые акты и стандарты.

Российские правовые акты в большинстве своем имеют ограничительную направленность. Но то, что для Уголовного или Гражданского кодекса естественно, по отношению к Закону об информации, информатизации и защите информации является принципиальным недостатком. Сами по себе лицензирование и сертификация не обеспечивают безопасности. К тому же в законах не предусмотрена ответственность государственных органов за нарушения ИБ. Реальность такова, что в России в деле обеспечения ИБ на помощь государства рассчитывать не приходится.

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

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

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

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

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

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

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

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

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

На втором месте по размеру ущерба стоят кражи и подлоги.

Реальную опасность представляют пожары и другие аварии поддерживающей инфраструктуры.

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

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

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

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

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

- инициация;

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

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

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

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

На этом уровне применимы важные принципы безопасности:

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

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

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

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

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

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

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

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

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

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

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

Программно-технические меры

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

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

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

Меры безопасности целесообразно разделить на следующие виды:

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

В продуманной архитектуре безопасности все они должны присутствовать.

С практической точки зрения важными также являются следующие принципы архитектурной безопасности:

- непрерывность защиты в пространстве и времени, невозможность миновать защитные средства;
- следование признанным стандартам, использование апробированных решений;
- иерархическая организация ИС с небольшим числом сущностей на каждом уровне;
- усиление самого слабого звена;
- невозможность перехода в небезопасное состояние;
- минимизация привилегий;
- разделение обязанностей;
- эшелонированность обороны;
- разнообразие защитных средств;
- простота и управляемость информационной системы.

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

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- шифрование;
- контроль целостности;
- экранирование;
- анализ защищенности;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелирование;
- управление.

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

Выделим важнейшие моменты для каждого из перечисленных сервисов безопасности:

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

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

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

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

Экранирование - идейно очень богатый сервис безопасности. Его реализации - это не только межсетевые экраны, но и ограничивающие интерфейсы, и виртуальные локальные сети. Экран инкапсулирует защищаемый объект и контролирует его внешнее представление. Современные межсетевые экраны достигли очень высокого уровня защищенности, удобства использования и администрирования; в сетевой среде они являются первым и весьма мощным рубежом обороны. Целесообразно применение всех видов МЭ - от персонального до внешнего корпоративного, а контролю подлежат действия как внешних, так и внутренних пользователей.

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

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

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

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

Миссия обеспечения информационной безопасности трудна, во многих случаях трудно выполнима, но всегда благородна.

Литература и первоисточники:

1. Classifying information for security. // In : DataPro on information security, 1989, IS15-250-101 - 106.
2. Orlandi Eug. Developing security awareness : explicative concepts for managers and end-users, // IFIP international conference on computer security, 1989, p. 411-420.
3. R.L.Rivest, A.Shamir and L.Adleman, "A method for obtaining digital signatures and public key cryptosystems". Com-mun. ACM,vol.21,pp120-126,1978
4. W.Diffie and M.E.Hellman, "New directions in cryptography", IEEE Trans.Inf.Theory, vol.IT-22, N6, pp644-654,Nov.1976
5. Wong K. Computer-related Fraud in UK, // Information Age, 1993. v.1, N 4, p. 2-9.
6. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: “Гелиос АРБ”, 2002г. - 480 с.
7. Барсуков В.С., Дворянкин С.В., Шеремет И.А. Безопасность связи в каналах телекоммуникаций. /Технологии электронных коммуникаций Том.20 / М., 1992г.
8. Батурин Ю. М., Жодзинский А. М. Компьютерная преступность и компьютерная безопасность. М.:"Юридическая литература" 1991 г. - 160 с.
9. Брассар Ж.Современная криптология. Пер.с англ. под ред. Лебедева А.Н. -М.: Издательско-полиграфическая фирма ПОЛИМЕД. 1999.- 176с.
10. Быков С.Ф. Мотуз О. В. Основы стегоанализа "Защита информации Конфидент" N 3 2000г с 38-41
11. Гайкович В., Першин А. Безопасность электронных банковских систем. Изд-во "Единая Европа" М. 1994г -364с.
12. Галатенко В.А. Информационная безопасность - грани практического подхода. http://www.citforum.ru/
13. Генне О.В. Основные положения стеганографии "Защита информации Конфидент" N 3 2000г с 20-25
14. Герасименко В. А., Малюк А.А. Основы защиты информации М.,1994г. 540с.
15. Голубев В. РАССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ Выступление 26 февраля 2003 г. на Southeast Cybercrime Summit в Атланте, США
16. Грязнов Е., Панасенко С. БЕЗОПАСНОСТЬ ЛОКАЛЬНЫХ СЕТЕЙ Мир и безопасность № 2, 2003
17. Девянин П.Н.,Михальский О.О.,ПравиковД.И., Щеобаков А.Ю.Теоретические основы компьютерной безопасности. Учебное пособие для вузов-М.:Радио и связь, 2000.-192с.
18. Дориченко С.А., Ященко В.В. 25 этюдов о шифрах. М. "ТЕИС" 1994г
19. Жуков Н.С., Кораблев А.Ю., Мельников Ю.Н. Информационная безопасность на объекте информатизации банка. Практическое руководство. Вестник Ассоциации Российских банков N 27-33 Москва 1997
20. Задорожный В. Обзор биометрических технологий Конфидент № 5 (53), 2003
21. Клочко В.А., Сабынин В.Н. Окомплексном подходе к обеспечению безо-пасности информации на телекоммунникационных объектах "Информост. Средства связи" N 1(14) 2001г с 19-22.
22. Козье Д. Электронная коммерция: Пер.с англ. -М.: Издательско-торговый дом "Русская Редакция". 1999.-288с.
23. Крумова М.А., Мельников Ю.Н., Райлян М.П. Подход к обеспечению живучести вычислительных систем телеобработки // Тез. докл. - НТ конференция с международным участием "Системы и средства телеобработки данных`89". - В.Тырново: 1989. с.49-55.
24. Кустов,В. Н., Федчук А. А., Методы встраивания скрытых сообщений "Защита информации Конфидент" N 3 2000г с 34-37
25. Медведовский И., Семьянов П., Платонов В. Атака через Internet. Под научной редакцией проф. Зегжды П.Д. – СПб.: "Мир и Семья – 95", 1997. – 296 с.
26. Мельников Ю. Н., Мясников В. А. Лутковский Ю. П. Обеспечение целостности информации в вычислительных системах. Известия АН СССР "Техническая кибернетика" N 1, 1985, с. 72 - 79
27. Мельников Ю.Н. Общие принципы защиты банковской информации. "Банковские технологии" N 7 1995 г. с.21-27
28. Мельников Ю.Н. Учебное пособие по курсу МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ (Кафедра комплексной защиты объектов информации)
29. Мельников Ю.Н. Электронная Цифровая Подпись - Электронная ЦифроваяПодпись: всегда ли она подлинная? "Банковские технологии" N 5 1995г. с.56-61.
30. Мельников Ю.Н., Баршак А.Д. Егоров П.Е. Сокрытие банковской информации нестандартными способами - Банковские технологии N 9 2001г с 25-29
31. Мельников Ю.Н., Егоров П.Е. Способ обнаружения скрываемой в файлах- контейнерах банковской информации Банковские технологии N 2 2002г с 43-45
32. Мельников Ю.Н., Иванов Д.Ю. Многоуровневая безопасность в корпоративных сетях. Международный форум информатизации - 2000: Доклады международной конференции "Информационные средства и технологии". 17-19 октября 2000 г. В 3-х тт. Т. 2. - М.: Издательство "Станкин", 2000г., - 245 с.
33. Мельников Ю.Н., Кузовенков Д.А. Способ обнаружения скрываемой в файлах-контейнерах банковской информации. Банковские технологии №2(76) 2002г. С.43-45.
34. Мельников Ю.Н., Теренин А.А. Рекомендации по доказательству фактапиратского использования программного продукта. “Интеллектуальная собственность.” Авторское право и смежные права №8, 2002г., С.56-59.
35. Мельников Ю.Н., Теренин А.А., Иванов Д.Ю., Мзоков Д.К., Перевалов П.А. ЗАЩИТА ИНФОРМАЦИИ. Лабораторные работы. Методическое пособие по курсу “Защита информации”. - М.: Изд-во МЭИ, 2002. - 70 с.
36. Мельников Ю.Н., Теренин А.А., Иванов Д.Ю., Мзоков Д.Ю., Перевалов П.А. Защита информации. Лабораторные работы. Методическое пособие по курсу “Защита информации”. - М.: Изд-во МЭИ, 2002. - 95 с. Находится в редакции.
37. Рето Е.Хэни, Лэнс Дж.Хоффман Информационная война Институт инженерных и прикладных наук Университет Джорджа Вашингтона Вашингтон, декабрь 1995г http://www.seas.gwu.edu/student/reto/
38. Сабынин В. Организация пропускного режим – первый шаг к обеспечению безопасности и конфиденциальности информации Информост-радиоэлектроника и телекоммуникации, № 3(16), 2001
39. Савельев М. ВНУТРЕННИЙ СПАМ PCWeek/RE, №32, 2003
40. Соболева Т.А. Тайнопись в истории России (История криптографической службы России XVIII - начала XX веков). М.: "Международные отношения" 1994г - 384 с.
41. Спесивцев А.В. и др.Защита информации в персональных ЭВМ. М. : Радио и связь, ВЕСТА, 1992 г.
42. Теренин А.А. Анализ возможных атак на защищенный канал в открытой сети, созданный программным способом. Материалы XXII Конференции молодых ученых механико-математического факультета МГУ, г. Москва, 17-22 апреля 2000 г.

43. Теренин А.А., Мельников Ю.Н. Создание защищенного канала в открытой сети. Материалы семинара "Информационная безопасность – юг России", г. Таганрог, 28-30 июня 2000 г.
44. Федотов Н.Н. Защита информации Учебный курс HTML-версия (**http://www.college.ru/UDP/texts**)
45. Шнайер Брюс "Прикладная криптография: Протоколы, алгоритмы и исходные тексты на языке С". **http://beda.stup.ac.ru/psf/ziss/wmaster/books/security/crypto/3/index.html**
46. Шрамко В. Аппаратно-программные средства контроля доступа "PCWeek/RE", N9, 2003