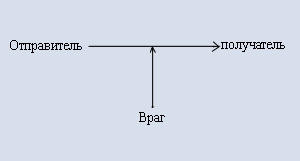
# Угрозы конфиденциальности

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги. В большинстве случаев злоумышленниками оказываются штатные сотрудники организаций (инсайдеры – люди, имеющие доступ к информации, недоступной для широкой публики), отлично знакомые с режимом работы и мерами защиты.

Конфиденциальную информацию можно разделить на **предметную** и **служебную**. *Служебная информация* (например, пароли пользователей) не относится к определённой предметной области, в ИС она играет техническую роль, но её раскрытие может быть особенно опасно, поскольку оно чревато получением несанкционированного доступа к предметной информации.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы её конфиденциальности могут носить некомпьютерный и вообще нетехнический характер. Многим людям приходится пользоваться не одним, а целым рядом информационных сервисов. Если для доступа к ним 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-трём легко запоминаемым (и столь же легко угадываемым) паролям.

**Перехват данных**



Возможность перехвата данных следует учитывать как при настройке, так и при всех изменениях конфигурации ИС. Опасной уязвимостью является размещение конфиденциальных данных в среде, где им не обеспечена необходимая защита: записанные пароли, передача конфиденциальных данных в открытом виде.

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 удалённом доступе они продолжают передаваться в открытом виде. Это плохо даже в пределах защищённой сети организации; в объединённой 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.

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.

Также угрозу представляют:

* Выставки.
* Хранение данных на резервных носителях.
* Межсайтовый скриптинг (XSS). Пример (для факультативного изучения).

XSS как дефект, при котором приложение включает в состав страницы, отправляемой пользователю, переданные им данные без их предварительной проверки или форматирования. Атаки на основе XSS на самом деле являются атаками на основе инъекций кода, затрагивающими процесс интерпретации отправленной веб-приложением страницы в пользовательском браузере.

Эти атаки в большинстве случаев проводятся в рамках систем онлайн-сообщений, блогов и пользовательских конференций (в совокупности называемых "системами онлайн-сообщений" в статье), в которых сообщения хранятся на постоянной основе. При их создании используются технологии HTML, JavaScript, VBScript, ActiveX, Flash и другие технологии сценариев на стороне клиентов.

Целью атак на основе межсайтового скриптинга является похищение пользовательских аутентификационных данных из кук и любой другой важной информации, которая участвует в процессе аутентификации клиента на веб-сайте. С похищенным (действительным) идентификатором пользователя взломщик может представиться пользователем и похитить его данные.

В отличие от большинства атак, в которых участвуют две стороны (взломщик и веб-сайт или взломщик и жертва/клиент), атака на основе межсайтового скриптинга предполагает участие трех сторон: взломщика, жертвы/клиента и веб-сайта.

В ходе атаки на основе межсайтового скриптинга действительному пользователю предоставляется ссылка, расположенная в системе онлайн-сообщений и ведущая на безопасный на первый взгляд сайт, но на самом деле содержащая закодированный сценарий, который выполняется как только пользователь переходит по ней. Этот на первый взгляд безопасный веб-сайт может быть (и является в большинстве случаев) клоном просматриваемого пользователем сайта для осуществления фишинг-атаки; в этом случае он запросит имя пользователя и пароль. В другом случае этот веб-сайт может представлять собой страницу с благодарностью, с помощью которой производится незаметное похищение кук пользователя в фоновом режиме.

**Кражи**

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.

**Методы социальной инженерии**

Опасной нетехнической угрозой конфиденциальности являются методы морально-психологического воздействия (социальная инженерия).

**Маскарад** — выполнение действий под видом лица, обладающего полномочиями для доступа к данным.

Целью «маскарада» является приписывание каких-либо действий другому пользователю либо присвоение полномочий и привилегий другого пользователя. Примерами реализации «маскарада» являются:  
• вход в систему под именем и паролем другого пользователя (этому «маскараду» предшествует перехват пароля);  
• передача сообщений в сети от имени другого пользователя.

«Маскарад» особенно опасен в банковских системах электронных платежей, где неправильная идентификация клиента из-за «маскарада» злоумышленника может привести к большим убыткам законного клиента банка.

Незаконное использование привилегий. Большинство систем защиты устанавливают определенные наборы привилегий для выполнения заданных функций. Каждый пользователь получает свой набор привилегий: обычные пользователи — минимальный, администраторы — максимальный. Несанкционированный захват привилегий, например посредством «маскарада», приводит к возможности выполнения нарушителем определенных действий в обход системы защиты. Следует отметить, что незаконный захват привилегий возможен либо при наличии ошибок в системе защиты, либо из-за халатности администратора при управлении системой и назначении привилегий.

**Фишинг (phishing)** — буквально «рыбалка», т. е. выуживание информации.

Рассмотрим некоторые популярные методики фишинга. Иногда они комбинируются с другими видами атак (например, с фармингом, вредоносным ПО).

1. Рассылка писем с сообщением о проблемах в БД интернет-провайдера, банка, системы электронной почты и т. д. и просьбой выслать некоторую информацию для восстановления.
2. Рассылка писем с сообщением о поступлении на счёт некоторой суммы и ссылкой на сайт фишеров.
3. Рассылка спама с рекламой однодневного интернет-магазина.
4. Применение трояна для перенаправления пользователя на сайт фишеров при попытке доступа к легитимному сайту (например, путём модификации файла hosts).
5. Сообщение об ошибке в электронной платёжной системе, воспользоваться которой можно, отправив определённую сумму на указанный кошелёк.
6. Генераторы номеров кредитных карт или системы скрытого списания денег с чужих счетов, в которых необходимо ввести номер и пароль своей карты.
7. Утилиты взлома чужого электронного ящика (hoax.win32.delf.g), в которых необходимо ввести свой адрес и пароль.
8. Генераторы кодов карт оплаты сотовой связи или Интернета, где в качестве «образца» нужно ввести код неактивированной карты.
9. Ввод учётных данных (имя, пароль) на другом сайте, который представлен как сайт-партнёр. Браузеры Internet Explorer 7 и Firefox 2 содержат встроенные средства проверки открываемого сайта по базе фишеров.

Из-за угрозы фишинга постоянно откладывается введение национальных алфавитов в доменных именах.

**Злоупотребление полномочиями**

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. Во многих типах ИС 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.