Республика Таджикистан

**Методы защиты информации в государственных информационных системах**

Халимов Джамшед

г. Душанбе

Современное состояние процессов реализации системы защиты информации, которая связанна с развитием информационно-коммуникационных технологий постепенно приводит к разрушению старой системы и требует новизны. Изменение же структуры и процессов защиты информации можно отнести к направлению, которая вынуждена реформироваться с развитием государственных информационных систем. Исходя из этих исходных положений, можно выразить основу защиты информации, которая должна составлять постоянную готовность системы защиты в любое время к отражению угроз информационной системы, активность прогнозирование действий, разработку и реализацию определенных мер по ее защите, сосредоточение усилий по предотвращению угроз наиболее ценной информации. Эти принципы определяют общие требования к способам и средствам защиты информации. В условиях развивающегося Таджикистана актуально, использовать на уровни организаций производящий интерес в решении задач отнесенной к защите собственной информации составляющий конфиденциальный характер методы Шифрования и Перестановки, а затем и на высоком уровне и средства Криптографии.

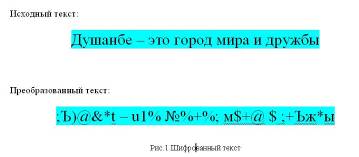
Метод Шифрование можно растолковать следующим образом:

Шифрование - способ преобразования открытой информации в закрытую и обратно. Применяется для хранения важной информации в ненадёжных источниках или передачи её по незащищённым каналам связи. Метод шифрование можно разделить на процесс зашифрования и расшифрования. Она выполняется таким образом:

Одна буква текста или слова при помощи ключа однозначно заменяется на другую или на определенный символ, то есть если у вас есть слово, которую необходимо зашифровать вы выполняете следующее действие:

1. Вначале устанавливаете для себя, как и какие буквы должны быть зашифрованы символами. К примеру буква **А** на **?**;
2. Отправляете ключ получателю, в том случае если вы намерены в ближайшее время отправить текст;
3. Выбираете слово, текст или предложение для шифрования;
4. Шифруете слово и передаете получателю;
5. Согласно переданному ключу получатель слова его расшифрует

Этот процесс можно указать на примере рис.1



В зависимости от порядка и структуры используемых ключей преобразование данных, методы шифрования подразделяются на два типа: временные и долговременные.

*Временные типы шифрования* используются в тех организациях, в которых несколько человек имеют доступ к информации и всегда есть угрозы его расшифрования, поэтому временные ключи для определенных лиц получателей информации постоянно изменяются отправителями.

*Долговременные типы* предназначены для обмена информацией на дальних расстояниях с целью шифрования от посторонних или третьих лиц передающихся данных. Долговременные шифрования используются в тех системах и устройствах, в которых не допускается изменения содержимого текста.

Существует ряд других не развитых, но развивающихся типов шифрования как:

*Архивное шифрование* - шифрование информации для хранения в защищенном виде, не преобразующемся и поддающаяся к обработки и изменению. В основном этот тип используется для долговременного хранения конфиденциальной информации. В современных условиях этот тип преобразуется в электронный носитель.

*Абонентское шифрование* - шифрование информации для последующей передачи по сети определенным пользователям (абонентам). Наиболее распространенный вид в экономически развитых государствах пока не применяющихся в государственном секторе передачи данными.

*Шифрование методом перестановки*

Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Если после замены символы сообщения превращались во что угодно, но сохраняли в шифровке свое исходное местоположение, после перестановки они там расположены еще и где угодно, что надежно защищает шифровку от атак.

Простейшим примером перестановки является запись исходного текста по строкам некоторой матрицы, а чтение его по строкам этой матрицы. Последовательность заполнения строк и чтения столбцов может быть любой и задается ключом.

Слабость шифрования простой перестановкой обуславливается тем, что при большой длине шифруемого текста в зашифрованном тексте могут появиться закономерности символов ключа. Для устранения этого недостатка можно менять ключ после зашифровки определенного числа знаков. При достаточно частой смене ключа стойкость шифрования можно существенно повысить. При этом, однако, усложняется организация процесса шифрования и расшифрования.

Существуют более сложные методы перестановки. Усложнение перестановки по таблице заключается в том, что для записи символов шифруемого текста используется специальная таблица, в которую введены некоторые усложняющие элементы. Пример такой таблицы приведен на рис. 2.



Следовательно, в условиях Таджикистана было бы эффективным способом защиты конфиденциальной информации Временным и Долговременным типом Шифрования, что является наиболее эффективным для развивающегося государства. Прежде для осуществления этого направления следует отобрать несколько организаций и установить между ними канал передачи шифрованной информации от отправителя к получателю. Настоящий процесс определит скорость передачи информации от отправителя к получателю, имеющему ключ расшифровки, а также защитить от посторонних лиц которым может быть известна содержание текста в зависимости от типа предлагаемого Шифрования.

Комбинированием этих методов можно добиться относительно хорошей защищенности информации. Невозможно абсолютно защитить информацию от несанкционированного доступа (взлома). Любой из этих способов поддается взлому в некоторой степени и, как правило, таких мер защиты информации иногда оказывается недостаточно, так как существует возможность, что некий преступник ночью заберется в офис фирмы и спокойно перепишет всю информацию. Поэтому существует ряд средств защиты, к которым согласно законодательству Республики Таджикистан можно отнести:

- организационные;

- технические;

- программные;

- аппаратные;

- физические;

- криптографические.

При реализации и использовании этих средств защиты необходимо, прежде всего, определить объект защиты (в нашем случае это значимая информация или документированная информация) по отношению к которой установлены определенные правила и ограничения в ее использовании.

Прежде чем использовать тот или иной метод необходимо узнать откуда поступает угроза и как с ней бороться, потому что, не зная источника, не можем использовать методику или средство защиты.

# *Угроза информации*

Угроза — это потенциальная возможность определенным образом нарушить информационную безопасность информационных систем или технологию работающею с системой.

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, которые в свою очередь могут быть как внутренними, так и внешними).

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 информационную среду, защита которых должна предприниматься в комплексном виде для временного или частичного блока и безопасности используемых данных.

Если речь идет об ошибках в программном обеспечении, то окно опасности «открывается» с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих, но и это не дает гарантии о полной защите и безопасности средств информации и информационных систем в целом.

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 информационной системе и т.д.

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 информационных систем и могут проявляться в любом виде и в любом месте используемой системы. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения информационной системы и от качественного электропитания его блоком питания.

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.

Подчеркнем, что 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 информационной безопасности, 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, землетрясение) 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 информационной системы).

В качестве основного критерия мы будем использовать первый (по аспекту информационной безопасности), 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 информационных систем, 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.

Таким образом, прежде чем защищать свою информацию пользователю необходимо уточнить источник и степень угрозы информации.