Реферат

На тему:

**"Обзор возможных методов защиты"**

# Содержание.

Содержание. 2

Обзор различных методов защиты информации 4

1. Причины влияющие на развитие в области защиты информации. 4

2. Методы защиты информации. 5

а) аппаратные методы защиты. 5

б) программные методы защиты. 6

в) резервное копирование. 6

г) криптографическое шифрование информации. 7

д) физические меры защиты. 9

е) организационные мероприятия по защите информации. 9

Заключение. 11

Литература. 12

#  Введение.

В последние годы в зарубежной, особенно в американской печати, большое внимание уделяется вопросам защиты информации, накапливаемой, хранимой и обрабатываемой в ЭВМ и построенных на их основе вычислительных системах. При этом под защитой информации понимается создание в ЭВМ и вычислительных системах организованной совокупности средств, методов и мероприятий, предназначенных для предупреждения искажения, уничтожения или несанкционированного использования защищаемой информации.

# Обзор различных методов защиты информации

## Причины влияющие на развитие в области защиты информации.

Содержание проблемы защиты информации специалистами интерпретируются следующим образом. По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается ее уязвимость. Основными факторами, способствующими повышению этой уязвимости, являются:

1. Резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ЭВМ и других средств автоматизации.
2. Сосредоточение в единых базах данных информации различного назначения и различных принадлежностей.
3. Резкое расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и находящимся в ней данных.
4. Усложнение режимов функционирования технических средств вычислительных систем: широкое внедрение многопрограммного режима, а также режимов разделения времени и реального времени.
5. Автоматизация межмашинного обмена информацией, в том числе и на больших расстояниях.

В этих условиях возникает уязвимость двух видов: с одной стороны, возможность уничтожения или искажения информации (т.е. нарушение ее физической целостности), а с другой - возможность несанкционированного использования информации (т.е. опасность утечки информации ограниченного пользования). Второй вид уязвимости вызывает особую озабоченность пользователей ЭВМ.

Основными потенциально возможными каналами утечки информации являются:

1. Прямое хищение носителей и документов.
2. Запоминание или копирование информации.
3. Несанкционированное подключение к аппаратуре и линиям связи или незаконное использование "законной" (т.е. зарегистрированной) аппаратуры системы (чаще всего терминалов пользователей).
4. Несанкционированный доступ к информации за счет специального приспособления математического и программного обеспечения.

## Методы защиты информации.

Можно выделить три направления работ по защите информации: теоретические исследования, разработка средств защиты и обоснование способов использования средств защиты в автоматизированных системах.

В теоретическом плане основное внимание уделяется исследованию уязвимости информации в системах электронной обработки информации, явлению и анализу каналов утечки информации, обоснованию принципов защиты информации в больших автоматизированных системах и разработке методик оценки надежности защиты.

К настоящему времени разработано много различных средств, методов, мер и мероприятий, предназначенных для защиты информации, накапливаемой, хранимой и обрабатываемой в автоматизированных системах. Сюда входят аппаратные и программные средства, криптографическое закрытие информации, физические меры организованные мероприятия, законодательные меры. Иногда все эти средства защиты делятся на технические и нетехнические, причем, к техническим относят аппаратные и программные средства и криптографическое закрытие информации, а к нетехническим - остальные перечисленные выше.

### а) аппаратные методы защиты.

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства. К настоящему времени разработано значительное число аппаратных средств различного назначения, однако наибольшее распространение получают следующие:

-специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности,

-генераторы кодов, предназначенные для автоматического генерирования идентифицирующего кода устройства,

-устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации,

-специальные биты секретности, значение которых определяет уровень секретности информации, хранимой в ЗУ, которой принадлежат данные биты,

-схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.

Особую и получающую наибольшее распространение группу аппаратных средств защиты составляют устройства для шифрования информации (криптографические методы).

### б) программные методы защиты.

К программным средствам защиты относятся специальные программы, которые предназначены для выполнения функций защиты и включаются в состав программного обеспечения систем обработки данных. Программная защита является наиболее распространенным видом защиты, чему способствуют такие положительные свойства данного средства, как универсальность, гибкость, простота реализации, практически неограниченные возможности изменения и развития и т.п. По функциональному назначению их можно разделить на следующие группы:

-идентификация технических средств (терминалов, устройств группового управления вводом-выводом, ЭВМ, носителей информации), задач и пользователей,

-определение прав технических средств (дни и время работы, разрешенные к использованию задачи) и пользователей,

-контроль работы технических средств и пользователей,

-регистрация работы технических средств и пользователей при обработки информации ограниченного использования,

-уничтожения информации в ЗУ после использования,

-сигнализации при несанкционированных действиях,

-вспомогательные программы различного назначения: контроля работы механизма защиты, проставления грифа секретности на выдаваемых документах.

### в) резервное копирование.

Резервное копирование информации заключается в хранении копии программ на носителе: стримере, гибких носителях, оптических дисках, жестких дисках. На этих носителях копии программ могут находится в нормальном (несжатом) или заархивированном виде. Резервное копирование проводится для сохранения программ от повреждений (как умышленных, так и случайных), и для хранения редко используемых файлов.

При современном развитии компьютерных технологий требования к запоминающим устройствам в локальной сети растут гораздо быстрее, чем возможности. Вместе с геометрическим ростом емкости дисковых подсистем программам копирования на магнитную ленту за время, отпущенное на резервирование, приходится читать и записывать все большие массивы данных. Еще более важно, что программы резервирования должны научиться таким образом управлять большим количеством файлов, чтобы пользователям не было чересчур сложно извлекать отдельные файлы.

Большинство наиболее популярных современных программ резервирования предоставляют, в том или ином виде, базу данных о зарезервированных файлах и некоторую информацию о том, на какой ленте находятся последние зарезервированные копии. Гораздо реже встречается возможность интеграции (или по крайней мере сосуществования) с технологией структурированного, или иерархического хранения информации (HSM, Hierarchical Storage Management).

HSM помогает увеличить емкость доступного пространства жесткого диска на сервере за счет перемещения статичных файлов (к которым последнее время не обращались) на менее дорогие альтернативные запоминающие устройства, такие как оптические накопители или накопители на магнитной ленте. HSM оставляет на жестком диске фиктивный файл нулевой длины, уведомляющий о том, что реальный файл перенесен. В таком случае, если пользователю потребуется предыдущая версия файла, то программное обеспечение HSM сможет быстро извлечь его с магнитной ленты или с оптического накопителя.

### г) криптографическое шифрование информации.

Криптографическое закрытие (шифрование) информации заключается в таком преобразовании защищаемой информации, при котором по внешнему виду нельзя определить содержание закрытых данных. Криптографической защите специалисты уделяют особое внимание, считая ее наиболее надежной, а для информации, передаваемой по линии связи большой протяженности, - единственным средством защиты информации от хищений.

Основные направления работ по рассматриваемому аспекту защиты можно сформулировать таким образом:

-выбор рациональных систем шифрования для надежного закрытия информации,

-обоснование путей реализации систем шифрования в автоматизированных системах,

-разработка правил использования криптографических методов защиты в процессе функционирования автоматизированных систем,

-оценка эффективности криптографической защиты.

К шифрам, предназначенным для закрытия информации в ЭВМ и автоматизированных системах, предъявляется ряд требований, в том числе: достаточная стойкость (надежность закрытия), простота шифрования и расшифрования от способа внутримашинного представления информации, нечувствительность к небольшим ошибкам шифрования, возможность внутримашинной обработки зашифрованной информации, незначительная избыточность информации за счет шифрования и ряд других. В той или иной степени этим требованиям отвечают некоторые виды шифров замены, перестановки, гаммирования, а также шифры, основанные на аналитических преобразованиях шифруемых данных.

Шифрование заменой (иногда употребляется термин "подстановка") заключается в том, что символы шифруемого текста заменяются символами другого или того же алфавита в соответствии с заранее обусловленной схемой замены.

Шифрование перестановкой заключается в том, что символы шифруемого текста переставляются по какому-то правилу в пределах какого-то блока этого текста. При достаточной длине блока, в пределах которого осуществляется перестановка, и сложном и неповторяющемся порядке перестановке можно достигнуть достаточной для практических приложений в автоматизированных системах стойкости шифрования.

Шифрование гаммированием заключается в том, что символы шифруемого текста складываются с символами некоторой случайной последовательности, именуемой гаммой. Стойкость шифрования определяется главным образом размером (длиной) неповторяющейся части гаммы. Поскольку с помощью ЭВМ можно генерировать практически бесконечную гамму, то данный способ считается одним из основных для шифрования информации в автоматизированных системах. Правда, при этом возникает ряд организационно-технических трудностей, которые, однако, не являются не преодолимыми.

Шифрование аналитическим преобразованием заключается в том, что шифруемый текст преобразуется по некоторому аналитическому правилу (формуле). Можно, например, использовать правило умножения матрицы на вектор, причем умножаемая матрица является ключом шифрования (поэтому ее размер и содержание должны сохранятся в тайне), а символы умножаемого вектора последовательно служат символы шифруемого текста.

Особенно эффективными являются комбинированные шифры, когда текст последовательно шифруется двумя или большим числом систем шифрования (например, замена и гаммирование, перестановка и гаммирование). Считается, что при этом стойкость шифрования превышает суммарную стойкость в составных шифрах.

Каждую из рассмотренных систем шифрования можно реализовать в автоматизированной системе либо программным путем, либо с помощью специальной аппаратуры. Программная реализация по сравнению с аппаратной является более гибкой и обходится дешевле. Однако аппаратное шифрование в общем случае в несколько раз производительнее. Это обстоятельство при больших объемах закрываемой информации имеет решающее значение.

### д) физические меры защиты.

Следующим классом в арсенале средств защиты информации являются физические меры. Это различные устройства и сооружения, а также мероприятия, которые затрудняют или делают невозможным проникновение потенциальных нарушителей в места, в которых можно иметь доступ к защищаемой информации. Чаще всего применяются такие меры:

-физическая изоляция сооружений, в которых устанавливается аппаратура автоматизированной системы, от других сооружений,

-ограждение территории вычислительных центров заборами на таких расстояниях, которые достаточны для исключения эффективной регистрации электромагнитных излучений, и организации систематического контроля этих территорий,

-организация контрольно-пропускных пунктов у входов в помещения вычислительных центров или оборудованных входных дверей специальными замками, позволяющими регулировать доступ в помещения,

-организация системы охранной сигнализации.

### е) организационные мероприятия по защите информации.

Следующим классом мер защиты информации являются организационные мероприятия. Это такие нормативно-правовые акты, которые регламентируют процессы функционирования системы обработки данных, использование ее устройств и ресурсов, а также взаимоотношение пользователей и систем таким образом, что несанкционированный доступ к информации становится невозможным или существенно затрудняется. Организационные мероприятия играют большую роль в создании надежного механизма защиты информации. Причины, по которым организационные мероприятия играют повышенную роль в механизме защиты, заключается в том, что возможности несанкционированного использования информации в значительной мере обуславливаются нетехническими аспектами: злоумышленными действиями, нерадивостью или небрежностью пользователей или персонала систем обработки данных. Влияние этих аспектов практически невозможно избежать или локализовать с помощью выше рассмотренных аппаратных и программных средств, криптографического закрытия информации и физических мер защиты. Для этого необходима совокупность организационных, организационно-технических и организационно-правовых мероприятий, которая исключала бы возможность возникновения опасности утечки информации подобным образом.

Основными мероприятиями в такой совокупности являются следующие:

-мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров (ВЦ),

-мероприятия, осуществляемые при подборе и подготовки персонала ВЦ (проверка принимаемых на работу, создание условий при которых персонал не хотел бы лишиться работы, ознакомление с мерами ответственности за нарушение правил защиты),

-организация надежного пропускного режима,

-организация хранения и использования документов и носителей: определение правил выдачи, ведение журналов выдачи и использования,

-контроль внесения изменений в математическое и программное обеспечение,

-организация подготовки и контроля работы пользователей,

Одно из важнейших организационных мероприятий - содержание в ВЦ специальной штатной службы защиты информации, численность и состав которой обеспечивали бы создание надежной системы защиты и регулярное ее функционирование.

# Заключение.

Основные выводы о способах использования рассмотренных выше средств, методов и мероприятий защиты, сводится к следующему:

1. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм защиты информации.
2. Механизм защиты должен проектироваться параллельно с созданием систем обработки данных, начиная с момента выработки общего замысла построения системы.
3. Функционирование механизма защиты должно планироваться и обеспечиваться наряду с планированием и обеспечением основных процессов автоматизированной обработки информации.
4. Необходимо осуществлять постоянный контроль функционирования механизма защиты.

# Литература.

1. Дж. Хоффман "Современные методы защиты информации"