**СОДЕРЖАНИЕ:**

Введение. 2

1. Факторы угроз сохранности информации в информационных системах. 4

2. Требования к защите информационных систем. 6

3. Классификация схем защиты информационных систем. 8

4. Анализ сохранности информационных систем. 13

5. Комплексная защита информации в персональных ЭВМ. 15

Заключение. 27

Список литературы: 28

# Введение.

Тема представленной работы – “Защита информационных систем”.

В качестве основных объективных причин, определяющих необходимость в изучении вопросов обеспечения сохранности информации, можно выделить следующие:

1. Высокие темпы роста парка ЭВМ, находящихся в эксплуатации. Парк ЭВМ количественно и качественно постоянно увеличивается.

2. Расширение областей использования ЭВМ. Широкое применение вычислительной техники в самых различных сферах человеческой деятельности объясняется рядом причин: развитием собственно вычислительной техники, которая позволяет решать задачи, связанные с управлением производством, различными технологическими процессами и системами, обработкой цифровой и символьной информации практически во всех областях науки и техники; постоянно возрастающем в соответствии с экспоненциальным законом объемом информации, который человек должен воспринимать и перерабатывать в процессе своей деятельности; более эффективным использованием трудовых и стоимостных ресурсов в экономике, возможностью решения новых научных проблем, принятия обоснованных решений на различных уровнях управления.

3. Высокая степень концентрации информации в центрах ее обработки. На современном этапе особое значение имеют банки данных, предназначенные для централизованного накопления и коллективного многоаспектного использования данных. Банк данных представляет собой человеко-машинную систему, включающую внутренних пользователей, в том числе и администрацию банка данных, а также технологию информационного процесса на базе ЭВМ и других средств вычислительной техники.

4. Количественное и качественное совершенствование способов доступа пользователя к ресурсам ЭВМ. Если к ЭВМ первого поколения имели доступ обслуживающий персонал и пользователи, находящиеся непосредственно в машинном зале, то современные СОД (системы обработки данных) могут обслуживать абонентов, удаленных на сотни и тысячи километров. Количество абонентов, пользующихся услугами системы одновременно, может быть очень большим. Стало возможным взаимное сопряжение различных ЭВМ при обмене информацией. Такие взаимосвязанные ЭВМ с подключенными к ним удаленными абонентскими терминальными устройствами образуют сложные информационно-вычислительные сети, распределенные на большой территории. Очевидно, что в этих системах такими организационными мерами, как поддержание строгого режима в помещениях, где установлены ЭВМ, исключить несанкционированный доступ к информации практически невозможно.

5. Усложнение вычислительного процесса на ЭВМ. Еще недавно ЭВМ работали в основном в однопрограммном режиме, т.е. сравнительно продолжительный период времени решалась только одна задача. Современные ЭВМ могут работать в мультипрограммном режиме (одновременно решается несколько задач), в мультипроцессорном режиме (создаются условия для решения программы задачи несколькими параллельно работающими процессорами), а также в режиме разделения времени, когда в одной и той же ЭВМ одновременно может обращаться большое количество абонентов. При таких режимах работы в памяти ЭВМ одновременно могут находиться программы и массивы данных различных пользователей, с ЭВМ одновременно будет поддерживать связь значительное число абонентов. В этом случае необходимо решение как проблем собственно физической защиты информации, так и сохранения информации от других пользователей или несанкционированного подключения пользователя, специально вклинивающегося в вычислительный процесс.

# 1. Факторы угроз сохранности информации в информационных системах.

**Умышленные факторы** сохранности информации в СОД зарубежные специалисты подразделяют на угрозы со стороны пользователей ЭВМ и лиц, не являющихся пользователями. Несанкционированный доступ к информации может включить неавторизованное пользование информацией системы и активную инфильтрацию. Неавторизованное пользование информацией отождествляется с ситуацией, когда неавторизованный пользователь получает возможность ознакомиться с информацией, хранимой в системе, и использовать ее в своих целях (прослушивание линий связи пользователей с ЭВМ, анализ информационных потоков, использование программ, являющихся чужой собственностью).

Под активной инфильтрацией информации подразумеваются такие действия, как просмотр чужих файлов через удаленные терминалы, маскировка под конкретного пользователя, физический сбор и анализ файлов на картах, магнитных лентах и дисках и т.д.

Намеренные попытки проникновения в СОД могут быть классифицированы как ***пассивные и активные***.

*Пассивное проникновение* - это подключение к линиям связи или сбор электромагнитных излучений этих линий в любой точке системы лицом, не являющимся пользователем ЭВМ.

*Активное проникновение* в систему представляет собой прямое использование информации из файлов, хранящихся в СОД. Такое проникновение реализуется обычными процедурами доступа: использованием известного способа доступа к системе или ее части с целью задания запрещенных вопросов, обращения к файлам, содержащим интересующую информацию; маскировкой под истинного пользователя после получения характеристик (идентификаторов) доступа; использованием служебного положения, т.е. незапланированного просмотра (ревизии) информации файлов сотрудниками вычислительной установки.

Активное проникновение в СОД может осуществляться скрытно, т.е. в обиход контрольных программ обеспечения сохранности информации.

*Наиболее характерные приемы проникновения*: использование точек входа, установленных в системе программистами, обслуживающим персоналом, или точек, обнаруженных при проверке цепей системного контроля; подключение к сети связи специального терминала, обеспечивающего вход в систему путем пересечения линии связи законного пользователя с ЭВМ с последующим восстановлением связи по типу ошибочного сообщения, а также в момент, когда законный пользователь не проявляет активности, но продолжает занимать канал связи; аннулирование сигнала пользователя о завершении работы с системой и последующее продолжение работы от его имени.

С помощью этих приемов нарушитель, подменяя на время его законного пользователя, может использовать только доступные этому пользователю файлы; неавторизованная модификация - неавторизованный пользователь вносит изменения в информацию, хранящуюся в системе. в результате пользователь, которому эта информация принадлежит, не может получить к ней доступ.

Понятие "неавторизованный" означает, что перечисленные действия выполняются вопреки указаниям пользователя, ответственного за хранение информации, или даже в обход ограничений, налагаемых на режим доступа в этой системе. Подобные попытки проникновения могут быть вызваны не только простым удовлетворением любопытства грамотного программиста (пользователя), но и преднамеренным получением информации ограниченного использования.

Возможны и ***другие виды нарушений***, приводящих к утрате или утечке информации. Так, электромагнитные излучения при работе ЭВМ и других технических средств СОД могут быть перехвачены, декодированы и представлены в виде битов, составляющих поток информации.

# 2. Требования к защите информационных систем.

Одно из существенных требований к системе обеспечения сохранности информации - отдельная идентификация индивидуальных пользователей, терминалов, индивидуальных программ (заданий) по имени и функции, а также данных при необходимости до уровня записи или элемента. Ограничить доступ к информации позволяет совокупность следующих способов: - иерархическая классификация доступа; - классификация информации по важности и месту ее возникновения; - указание специфических ограничений и приложение их к специфическим объектам, например пользователь может осуществлять только чтение файла без права записи в него; - содержание данных или отдельных групп данных (нельзя читать информацию по отдельным объектам); - процедуры, представленные только конкретным пользователям. Пользователи программ должны ограничиваться только одной или всеми привилегиями: чтением, записью, удалением информации.

При реализации записи предусматривается ее модификация (увеличение, уменьшение, изменение), наращивание ( элемента, записи, файла) и введение (элемента, записи, файла). Система обеспечения сохранности информации должна гарантировать, что любое движение данных идентифицируется, авторизуется, обнаруживается и документируется.

Организационные требования к системе защиты реализуются совокупностью административных и процедурных мероприятий. Требования по обеспечению сохранности должны выполняться прежде всего на административном уровне. С этой целью: - ограничивается несопровождаемый доступ к вычислительной системе (регистрация и сопровождение посетителей); - осуществляется контроль за изменением в системе программного обеспечения; - выполняется тестирование и верификация изменения в системе программного обеспечения и программах защиты; - организуется и поддерживается взаимный контроль за выполнением правил обеспечения сохранности данных; - ограничиваются привилегии персонала, обслуживающего СОД; - осуществляется запись протокола о доступе к системе; - гарантируется компетентность обслуживающего персонала.

Организационные мероприятия, проводимые с целью повышения эффективности обеспечения сохранности информации, могут включать следующие процедуры: - разработку последовательного подхода к обеспечению сохранности информации для всей организации; - организацию четкой работы службы ленточной и дисковой библиотек; - комплектование основного персонала на базе интегральных оценок и твердых знаний; - организацию системы обучения и повышения квалификации обслуживающего персонала.

С точки зрения обеспечения доступа к СОД необходимо выполнять следующие процедурные мероприятия: - разработать и утвердить письменные инструкции на запуск и останов системы; - контролировать использование магнитных лент, дисков, карт, листингов, порядок изменения программного обеспечения и доведение этих изменений до пользователя. - разработать процедуру восстановления системы при сбойных ситуациях; - установить политику ограничений при разрешенных визитах в вычислительный центр и определить объем выдаваемой информации; - разработать систему протоколирования использования ЭВМ, ввода данных и вывода результатов; - обеспечить проведение периодической чистки архивов и хранилищ лент, дисков, карт для исключения и ликвидации неиспользуемых; - поддерживать документацию вычислительного центра в соответствии с установленными стандартами.

# 3. Классификация схем защиты информационных систем.

Сохранность информации может быть нарушена в двух основных случаях: при получении несанкционированного доступа к информации и нарушении функционирования ЭВМ. система защиты от этих угроз включает следующие основные элементы: защиту СОД и ее аппаратуры, организационные мероприятия по обеспечению сохранности информации, защиту операционной системы, файлов, терминалов и каналов связи.

Следует иметь в виду, что все типы защиты взаимосвязаны и при выполнении своих функций хотя бы одной из них сводит на нет усилия других. Предлагаемые и реализованные схемы защиты информации в СОД очень разнообразны, что вызвано в основном выбором наиболее удобного и легко осуществимого метода контроля доступа, т.е. изменением функциональных свойств системы.

В качестве классификационного признака для схем защиты можно выбрать их **функциональные свойства**. На основе этого признака выделяются системы: без схем защиты, с полной защитой, с единой схемой защиты, с программируемой схемой защиты и системы с засекречиванием. В некоторых системах отсутствует механизм, препятствующий пользователю в доступе к какой-либо информации, хранящейся в системе. Характерно, что большинство наиболее распространенных и широко применяемых за рубежом СОД с пакетной обработкой не имеют механизма защиты. Однако такие системы содержат обычно развитый аппарат обнаружения и предотвращения ошибок, гарантирующий исключение разрушений режима функционирования.

**В системах с полной защитой** обеспечивается взаимная изоляция пользователей, нарушаемая только для информации общего пользования (например, библиотеки общего пользования). В отдельных системах средства работы с библиотеками общего пользования позволяют включить в них информацию пользователей, которая тоже становится общим достоянием.

**В системах с единой схемой защиты** для каждого файла создается список авторизованных пользователей. Кроме того, применительно к каждому файлу указываются разрешаемые режимы его использования: чтение, запись или выполнение, если этот файл является программой. Основные концепции защиты здесь довольно просты, однако их реализация довольно сложная.

**В системах с программируемой схемой защиты** предусматривается механизм защиты данных с учетом специфических требований пользователя, например, ограничение календарного времени работы системы, доступ только к средним значениям файла данных, локальная защита отдельных элементов массива данных и т.д. В таких системах пользователь должен иметь возможность выделить защищаемые объекты и подсистемы.

**Защищаемая подсистема** представляет собой cовокупность программ и данных, правом доступа к которым наделены лишь входящие в подсистему программы.Обращение к этим программам возможно, в свою очередь, только в заранее ограниченных точках. Таким образом, программы подсистемы контролируют доступ к защищаемым объектам. Подобный механизм защиты с различными модификациями реализован только в наиболее совершенных СОД.

**В системах с засекречиванием** решаются не вопросы ограничения доступа программ к информации, а осуществляется контроль над дальнейшим использованием полученной информации. Например, в системе использования грифов секретности на документах гриф служит уведомлением о мере контроля. В СОД эта схема защиты используется редко.

*Отличительная особенность рассмотренных схем защиты* - их динамичность, т.е. возможность ввода и изменения правил доступа к данным в процессе работы системы. Однако, обеспечение динамичности схем защиты значительно усложняет их реализацию.

Вопросы организации защиты информации должны решаться уже на предпроектной стадии разработки СОД.

Следует учитывать, что инфильтрация в систему будет возрастать с ростом значения доступа к информации ограниченного доступа. Именно на этой стадии необходимо четко представлять возможности потенциального нарушителя с тем, чтобы излишне не "утяжелить" систему. Опыт проектирования систем защиты еще недостаточен.

Однако уже можно сделать некоторые обобщения. Погрешности защиты могут быть в значительной мере снижены, если при проектировании учитывать следующие **основные принципы построения системы защиты.**

1. ***Простота механизма защиты***. Этот принцип общеизвестен, но не всегда глубоко осознается. Действительно, некоторые ошибки, не выявленные в ходе проектирования и реализации, позволяют найти неучтенные пути доступа. Поэтому необходимо тщательное тестирование программного или схемного аппарата защиты, но на практике такая проверка возможна только для простых и компактных схем. 2. В механизме ***защиты разрешения должны преобладать над запретами***. А это означает, что в нормальных условиях доступ должен отсутствовать и для работы схемы защиты необходимы условия, при которых доступ становится возможным. Кроме того считается, что запрет доступа при отсутствии особых указаний обеспечивает высокую степень надежности механизма защиты. Ошибка в схеме защиты, основанной на использовании разрешений, приводит к расширению сферы действия запретов. Эту ошибку легче обнаружить, и она не нарушит общего статуса защиты.

3. ***Контроль должен быть всеобъемлющим***. Этот принцип предполагает необходимость проверки полномочия любого обращения к любому объекту и является основой системы защиты. Задача управления доступом с учетом этого принципа должна решаться на общесистемном уровне и для таких режимов работы, как запуск, восстановление после сбоя, выключение и профилактическое обслуживание. При этом необходимо обеспечить надежное определение источника любого обращения к данным.

4. ***Механизм защиты может не засекречиваться***, т.е. не имеет смысла засекречивать детали реализации системы защиты, предназначенной для широкого использования. Эффективность защиты не должна зависеть от того, насколько опытны потенциальные нарушители, так как гораздо проще обеспечить защиту списка паролей (ключей).Отсутствие же связи между механизмом защиты и паролями позволяет сделать при необходимости схемы защиты предметом широкого обсуждения среди специалистов, не затрагивая при этом интересы пользователей.

5. Разделение полномочий, т.е. ***применение нескольких ключей защиты.*** В СОД наличие нескольких ключей защиты удобно в тех случаях, когда право на доступ определяется выполнением ряда условий.

6. ***Минимальные полномочия***. Для любой программы и любого пользователя должен быть определен минимальный круг полномочий, необходимых для выполнения порученной работы. Благодаря этим действиям в значительной мере уменьшается ущерб, причиняемый при сбоях и случайных нарушениях. Кроме того, сокращение числа обменов данными между привилегированными программами до необходимого минимума уменьшает вероятность непреднамеренного, нежелательного или ошибочного применения полномочий. Таким образом, если схема защиты позволяет расставить "барьеры" в системе, то принцип минимальных полномочий обеспечивает наиболее рациональное расположение этих "барьеров".

7. ***Максимальная обособленность механизма защиты***. В целях исключения обменов информацией между пользователями при проектировании схемы защиты рекомендуется сводить к минимуму число общих для нескольких пользователей параметров и характеристик механизма защиты. Несмотря на то, что функции операционной системы разрешения доступа перекрываются, система разрешения доступа должна конструироваться как изолированный программный модуль, т.е. защита должна быть отделена от функций управления данными. Выполнение этого принципа позволяет программировать систему разрешения доступа как автономный пакет программ с последующей независимой отладкой и проверкой. Пакет программ должен размещаться для работы в защищенном поле памяти, чтобы обеспечить системную локализацию попыток проникновения извне. Даже попытка проникновения со стороны программ операционной системы должна автоматически фиксироваться, документироваться и отвергаться, если вызов выполнен некорректно. Естественно, что в результате реализации обособленного механизма защиты могут возрасти объемы программы и сроки на ее разработку, возникнуть дублирование управляющих и вспомогательных программ, а также необходимость в разработке самостоятельных вызываемых функций.

8. ***Психологическая привлекательность.*** Схема защиты должна быть в реализации простой. Естественно, чем точнее совпадает представление пользователя о схеме защиты с ее фактическими возможностями, тем меньше ошибок возникает в процессе применения. Использование некоторых искусственных языков при обращении к схеме защиты обычно служит источником дополнительных ошибок.

# 4. Анализ сохранности информационных систем.

Анализ сохранности информационных систем основывается на постоянном изучении протоколов (как машинных, так и ручных), проверке аварийных сигнализаторов и других устройств. Важным фактором является также и то, что такой обзор поддерживает интерес к вопросам обеспечения сохранности.

За проведение анализа отвечает сотрудник, занимающийся вопросами обеспечения сохранности. Приборы аварийной сигнализации должны проверяться достаточно часто, но в случайные моменты времени. К их числу относятся детекторы огня и дыма, датчики влажности и температуры, аппаратура сигнализации при попытках проникновения в помещение, устройства физического контроля доступа, дверная сигнализация и другие аналогичные приборы. проводится также проверка состояния противопожарного оборудования, доступа к аварийным выходам и системам отключения электро-, водо- и теплоснабжения. Еженедельно проверяется исправность устройств и линий связи. Осматривается также пространство под технологическим полом и другие полости, в которых могут накапливаться отходы, создающие опасность самовозгорания, или вода при ее утечках. По проводимым работам ведется протокол проверки, каждая запись которого сопровождается замечаниями об отклонениях. Зарубежные специалисты считают, что этой работе должно отводиться около одного часа в неделю.

Другая важная и регулярная работа связана с изучением ручных и машинных протокольных записей. результаты регулярных проверок протоколов должны оформляться по определенному образцу с тем, чтобы не пропустить какой-либо вид проверки. Рекомендуется тщательно исследовать любые подозрительные тенденции и отклонения от принятых стандартов в работе.

Более того, описанные операции сами по себе являются объектом, сохранность которого необходимо обеспечить, поэтому должно быть выделено специальное помещение с терминалом, на котором выполняются только работы по обеспечению сохранности.

Побочным продуктом анализа сохранности может оказаться статистическая оценка эффективности использования оборудования организации и оценка эффективности работы пользователей. На основе результатов проверки проводятся еженедельные совещания руководителей организации, на котором заслушивается сообщение сотрудника, ответственного за обеспечение сохранности. Такие совещания позволяют оценить усилия по защите и выработать дополнительные рекомендации по совершенствованию принятых методов обеспечения сохранности.

Следует анализировать все возможности нарушения сохранности и отыскивать средства борьбы с ними. Если стандартные процедуры не выполняются, то повторяют инструктаж с целью выполнения этих процедур. Кроме обычных регулярных проверок, описанных выше, сотрудник, ответственный за обеспечение сохранности, обязан выполнять тестовый контроль проверки аппаратуры и программного обеспечения. Результаты тестирования фиксируются в специальном журнале. Это требует некоторых затрат ручного труда и машинного времени. В СОД, в которых уровень обеспечения сохранности высок, тестирование должно проводиться более часто и по возможности автоматически. Результаты тестирования также анализируются сотрудником, ответственным за обеспечение сохранности.

# 5. Комплексная защита информации в персональных ЭВМ.

По статистике более 80% компаний и агентств несут финансовые убытки из-за нарушения безопасности данных.

Многие фирмы сейчас занимаются разработкой различных антивирусных программ, систем разграничения доступа к данным, защиты от копирования и т.д. Объясняется это сравнительной простотой разработки подобных методов и в то же время достаточно высокой их эффективностью.

Рассмотрим основные механизмы реализации конкретных программных средств защиты информации.

***Программы-идентификаторы*** служат для контроля входа в ЭВМ, аутентификации пользователя по вводу пароля и разграничения доступа к ресурсам ЭВМ. Под идентификацией пользователя понимается процесс распознавания конкретного субъекта системы, обычно с помощью заранее определенного идентификатора; каждый субъект системы должен быть однозначно идентифицируем. А под аутентификацией понимается проверка идентификации пользователя, а также проверка целостности данных при их хранении или передаче для предотвращения несанкционированной модификации.

При загрузке с накопителя на жестком магнитном диске система BIOS выполняет считывание 1го сектора 0-го цилиндра 0-ой дорожки. Этот сектор называется "Главная загрузочная запись" - Master boot record /МВR/. Обычно программа, записанная в МВR, загружает запись BOOT RECORD /BR/ активного раздела. Однако можно использовать МВR для организации контроля входа в ПЭВМ. Так как размер программы МВК невелик, то на нее можно возложить очень ограниченные функции. Например, можно попробовать "уложить" в нее вместе с основной функцией и программу проверки пароля.

Однако эффективней использовать МВR для загрузки другой, большей по объему программы. При применении стандартной разбивки НЖМД на разделы с помощью программы FDISK сектора с номером, больше или равным 3, 0-ой дорожки 0-го цилиндра не используются, поэтому их можно применить для хранения большей по объему программы, выполняющей функции контроля. Помимо этого в записи МВR хранится первичная таблица описателей логических дисков. Изменение этой таблицы позволяет предотвратить доступ к логическому диску (разделу) на уровне системы DOS при загрузке с дискеты. Первый сектор активного раздела содержит загрузочную запись ВК, осуществляющую загрузку операционной системы. В начале этой записи содержится таблица параметров логического диска. BR может использоваться для загрузки не операционной системы, а некоторой другой программы, реализующей разграничения доступа. Эта программа в свою очередь должна в конце своей работы загрузить операционную систему. Объем ВR достаточен для размещения программы, реализующей загрузку произвольного файла из корневого каталога логического диска. Модификация таблицы параметров некоторого логического диска может использоваться и для предотвращения доступа к этому логическому диску при загрузке ЭОБ с дискеты.

Примером программ такого рода является система SHIELD, которая состоит из 2-х файлов: sset.com и sswith.com При первой установке системы файл sset.com копирует оригинальный МВR во 2-ой сектор 0-ой дорожки нулевого цилиндра, а в первом секторе оставляет модифицированный вариант МВR, который перед загрузкой DOS запрашивает пароль. Если пароль неверен, то жесткий диск оказывается недоступен. Для снятия защиты используется файл sswitch.com, который возвращает на место оригинальный сектор с МВR. Программы такого рода целесообразно использовать для защиты компьютера без НГМД, так как при загрузке с дискеты можно беспрепятственно читать и копировать данные с НЖМД.

Кроме того, для профессионала подобная защита не представляет серьезных затруднений. В стандартной среде DOS в качестве командного процессора используется COMMAND.СОМ. Однако система допускает установку другого командного процессора по команде SHELL в файле СОМГ10.БУБ. С помощью нового командного процессора можно разрешить запуск только определенных программ и запретить запуск других.

Написание нового командного процессора - задача достаточно сложная и не всегда оправданная, так как возможно решение тех же самых задач более простыми способами (написание драйвера или программы, запускаемой из файла AUTOEXEC. ВАТ). Пример командного процессора – файл PWLOAD.СОМ, разработанный 2В Рrogrammers Groups. Эта программа запрашивает пароль и, если он набран неверно, то работа ЭВМ блокируется.

Функции разграничения доступа также можно реализовать с помощью драйвера устройства, определяемого в файле CONFIG.SYS. Этот драйвер может контролировать доступ к файлам, каталогам и нестандартно определенным логическим дискам. Для этой цели обычно осуществляется перехват прерывания DOS INT 2lh и других прерываний операционной системы, организуется посекторная защита от чтения/ записи, защита от переименования и перемещения.

Это связано с определенными трудностями, так как необходимо хранить таблицы большого объема, описывающие полномочия по доступу к каждому сектору, и теневые таблицы FАТ и DIR для проверки корректности при их перезаписывании. В общем случае эта проблема представляется трудноразрешимой из-за большого объема данных, подлежащих хранению и обработке в системе разграничения доступа. На драйвер можно также возложить запрос пароля на вход в систему.

Существуют *драйверы для организации режима прозрачного шифрования данных на дисках*. Такой драйвер осуществляет перехват прерывания BIOS INT 13h, контролируя таким образом все операции с диском (чтение, запись и т.д. ) При этом данные на защищенном диске (или его разделе ) находятся в зашифрованном виде, а ключи могут храниться на нестандартно отформатированной ключевой дискете для большей безопасности данных. Такая мера защиты удобна для предотвращения чтения данных с НЖМД при загрузке с дискеты.

Но и здесь имеется ряд существенных недостатков. Во-первых, ключи шифрования хранятся в оперативной памяти, а потому могут быть считаны злоумышленниками. Во-вторых, всегда можно получить открытое содержимое файла, переписав его в некоторый файл, расположенный не в группе файлов прозрачного шифрования.

Пример драйвера - система DISKREET из пакета NORTON UTILITES: включает в себя файлы DISKREET.SYS и DISKREET.ЕХЕ. DISKREET.SYS драйвер, загружаемый из CONFIG.SYS и позволяющий создавать нестандартно определенные логические диски, защищенные паролем, которые к тому же зашифрованы по оригинальному алгоритму.

Программа DISKREET.ЕХЕ позволяет зашифровывать и расшифровывать любые файлы и каталоги на дисках. Программы, резидентные в памяти, могут выполнять те же функции, что и драйверы. Существует разница лишь при загрузке: драйвер загружается из CONFIG.SYS командой DEVICE, а резидентные программы из файла AUTOEXEC.ВАТ.

Кроме этого такие программы часто используются для контроля и предотвращения заражения компьютера вирусами. Примером такой программы может служить ревизор -V.СОМ из антивирусного пакета Е.Касперского.

**Программы-шифровальщики** выполняют только одну функцию - шифрование данных: файлов, каталогов и дисков по ключу, вводимому пользователем. Применяются самые разнообразные алгоритмы шифрования: от криптографически стойких DES и FEAL до тривиальных алгоритмов побитового сложения с ключом. Примеров таких программ достаточно много. К преимуществам программных средств защиты можно отнести их невысокую стоимость, простоту разработки. Недостатком таких систем является невысокая степень защищенности информации. Для усиления защиты можно предложить использование нескольких программных средств одновременно.

Например, использовать пароль при входе, систему разграничения доступа и режим прозрачного шифрования. При этом возникнут определенные неудобства в работе, но вместе с тем возрастет надежность.

Рассмотрим далее **основные виды программно - аппаратных средств защиты информации**. Они характеризуются более высокой стойкостью и, как следствие, более высокой стоимостью. Но при применении аппаратно-программных комплексов на предприятиях с повышенным риском появления угроз (например, на военных объектах или в коммерческих банках) затраты на установку такой защиты окупаются полностью. Многие фирмы - производители компьютеров предусматривают защиту их от несанкционированного доступа на уровне микросхемы ПЗУ с BIOS. Так, при загрузке компьютера при включении питания еще во время процедуры POST требуется указать правильный пароль, чтобы машина продолжала работу. Иногда возможность установки пароля реализована в BIOS, но не описана в документации. Некоторые вирусы могут записывать в поле пароля случайную информацию, и однажды пользователь обнаруживает, что его машина неплохо защищена от него. Сам пароль хранится в области CMOS и при большом желании может быть стерт. Фирма Сompaq пошла дальше и включила в BIOS программы, поддерживающие следующие области разделения доступа: возможность быстром запирания компьютера, защита жесткого диска, гибкого диска, последовательного и параллельного портов. Запуск защитных программ из BIOS регулируется переключателями на плате компьютера.

Следует отметить, что эффективность подобной защиты достигается только в сочетании с организационными мерами защиты, так как при наличии свободного доступа к "внутренностям" компьютера злоумышленнику не составит большого труда заменить микросхему с BIOS или разрядить батарею питания, нейтрализовав таким образом вышеперечисленные защитные меры. Шифрующая плата вставляется в слот расширения на материнской плате компьютера и выполняет функцию шифрования. Режим шифрования может быть прозрачным или предварительным. Могут шифроваться как отдельные файлы, так и каталоги или целые диски. На плате находится датчик псевдослучайных чисел для генерации ключей и узлы шифрования, аппаратно реализованные в специализированных однокристальных микроЭВМ. Ключи шифрования хранятся на специально созданной для этого дискете. Программная часть комплекса содержит драйвер платы для взаимодействия программ пользователя с платой шифрования.

В качестве примера рассмотрим продукт фирмы "АНКАД" - программно-аппаратный комплекс" Криптон " (версии 1,2,3,4). Данное устройство обеспечивает высокую криптографическую стойкость, шифрование производится по алгоритму ГОСТ 28174 - 89. Открытый интерфейс позволяет разрабатывать дополнительное программное обеспечение специального назначения. Длина ключа - 256 бит. Скорость шифрования - до 200 Кбайт/ сек. Аппаратные требования: IBM PC ХТ/АТ, MS-DOS 3,0 и выше. Программная поддержка позволяет осуществлять: шифрование файлов, разделов, дисков; разграничение и контроль доступа к компьютеру; электронную подпись юридических и финансовых документов; прозрачное шифрование жестких и гибких дисков. Шифровальные платы обладают высокой гарантией защиты информации, но их применение вносит определенные неудобства в работу ПЭВМ, прежде всего - это значительное снижение скорости обработки данных, а также необходимость инициализировать плату при каждом включении компьютера.

В последнее время широкое распространение получили **электронные ключи**. Это устройство подключается к компьютеру через порт LPT (есть модели, которые используют СОМ порт). При этом электронный ключ не мешает нормальной работе параллельного порта и полностью "прозрачен" для принтера и других устройств. Ключи могут соединяться каскадно, как правило, до 8 штук подряд. При этом в цепочке могут работать совершенно разнотипные ключи, выпущенные разными фирмами.

Электронные ключи могут выполнять различные функции. Например, защиту программ от несанкционированном копирования, при этом в исполняемый модуль -СОМ или -ЕХЕ файл встраиваются фрагменты кода для обмена с электронным ключом и управления им ( размер кода обычно не превышает 2 Кбайт ). Электронные ключи позволяют защищать не только -СОМ и -ЕХЕ программы, но и работать с неисполняемыми приложениями, например: AUTOCAD LISP , макросами электронных таблиц типа LOTUS , RUNTIME - модулями, интерпретаторами, базами данных, кодированными графическими файлами и т.п. Помимо основных защитных функций ключи многих фирм способны обнаруживать факт заражения защищенной программы различными видами файловых вирусов. Очень эффективно применение электронных ключей для хранения и передачи шифровальном ключа при применении различных методов шифрования (DES,DSS,RSA, ГОСТ и т.д.), поскольку хранение и передача ключей - самое слабое место в большинстве существующих алгоритмов. А при использовании электронных ключей для генерации шифровальных ключей отпадает необходимость их запоминать или записывать, а затем вводить с клавиатуры. Ключ не имеет встроенных источников питания и сохраняет записанную в него информацию при отключении от компьютера. В нашей стране наиболее распространены ключи американской фирмы "Software Security Inc". Эта фирма выпускает ключи для DOS, WINDOWS, UNIX, OS/2, Macintosh. Ключи могут быть как с одноразовой записью, так и перепрограммируемые; могут содержать энергонезависимую память или не содержать. Электронные ключи представляют собой одно из самых эффективных и удобных средств защиты от копирования.

***Пластиковые идентификационные карты (ИК)*** внедряются во многие сферы нашей жизни. Маленькие размеры карты, удобство хранения, достаточно высокий объем памяти делают ИК незаменимыми во многих областях человеческой деятельности.

Есть множество примеров использования ИК в СЗИ, например, для реализации защиты ПЭВМ от несанкционированного доступа. Такой аппаратно - программный комплекс состоит из аппаратной части: специальной платы, которая вставляется в слот расширения ПК, устройства считывания информации с ИК и самих ИК; также имеется программная часть: драйвер для управления платой и устройством считывания с ИК.

В программную часть комплекса может входить также программное обеспечение для организации разграничения доступа к частям и разделам жесткого диска. Кроме того система защиты запрашивает пароль. Таким образом исключается вход в систему по украденной карточке.

Пример аппаратно - программного комплекса защиты - разработка фирмы Datamedia. Серия ее компьютеров Netmate оборудована специальным устройством Securecard reader - считыватель карт безопасности. Карты безопасности по исполнению - вариант кредитных карт; на их магнитном носителе с помощью специальной аппаратуры, которая имеется только в распоряжении администратора, делается запись о пользователе: его имя, пароль и описываются все полномочия, которые он получает при входе в систему. В частности, на карте записано, сколько раз пользователь может пытаться указать пароль при входе. Таким образом, случайная потеря карты безопасности или ее кража не позволяет злоумышленнику получить доступ к компьютеру: если имя пользователя еще можно узнать, не привлекая внимания, то пароль ему неизвестен. Только сознательная передача карты безопасности кому-то одновременно с разглашением пароля может открыть доступ к компьютеру постороннему лицу.

Администратор системы создает карту безопасности для легальных пользователей. На этой карте помимо уже перечисленной информации описывается профиль пользователя. В нем включаются, например: возможность доступа к программе SETUP, то есть фиксируются такие характеристики компьютера, как экран, количество и типы дисков; также определяется, какие из локальных устройств ( гибкие диски, жесткие диски, последовательные и параллельные порты ) доступны этому пользователю, с каких локальных или сетевых устройств он может загружаться. Предусмотрена трансляция паролей: тот пароль, который назначается пользователю, как правило, легко запоминающийся, но вовсе не тот, с которым работает система. При попытке просто выдернуть карту безопасности из считывателя - доступ к компьютеру намертво блокируется, пока в считыватель не будет вставлена та же карта безопасности. При неправильном указании пароля (если превышено количество попыток, разрешенное для данного пользователя) - машина блокируется, и только администратор сможет "оживить" ее, то есть стимулируется необходимость довести до сведения администрации все случаи нарушения режима секретности.

С точки зрения **защиты от вирусов** перечисленные системы, тоже важны, поскольку они, кроме идентификации пользователя определенным образом организуют его работу на компьютере, запрещая отдельные опасные действия типа запуска программ с дискеты, загрузки с дискет. Ограничения на использование определенных ресурсов системы типа сетевых карт, последовательных портов также полезны с точки зрения защиты от вирусов, поскольку ограничивают возможность или даже отсекают некоторые пути распространения или получения заразы, Наконец, повышенный уровень тревоги, характерный для этой системы очень полезен и с антивирусной точки зрения: любые неполадки и странности в работе компьютеров немедленно должны становиться достоянием администрации и также немедленно доводиться до сведения специалистов, что резко уменьшает размеры ущерба от проникновения вирусов.

ИК могут использоваться и для хранения ключей шифрования в системах криптографической защиты.

Недостатком такой системы является низкая защищенность ИК с магнитной полосой. Как показывает опыт, информация с них может быть беспрепятственно считана. А применение ИК со встроенным чипом из-за высокой стоимости таких ИК ведет к значительному увеличению затрат на установку системы защиты, Кроме того, дорого обходится и оборудование для считывания информации с ИК. Но, несмотря на высокую стоимость, системы защиты на базе ИК находят широкое применение там, где необходима высокая надежность, например, в коммерческих структурах.

В настоящее время большую популярность завоевало *семейство приборов Touch memory (ТМ)*, производимое фирмой Dallas Semiconductods.

Данный выбор был определен прежде всего высокой надежностью, поскольку вывести touch-memory из строя достаточно трудно. Одним из основных отличий приборов Touch Memory от других компактных носителей информации является конструкция корпуса. Помимо защиты стальной корпус выполняет также роль электрических контактов. Приемлемы и массо-габаритные характеристики - таблетка диаметром с двухкопеечную монету и толщиной 5 мм очень подходит для таких применений. Каждый прибор семейства является уникальным, так как имеет свой собственный серийный номер, который записывается в прибор с помощью лазерной установки во время его изготовления и не может быть изменен в течение всего срока службы прибора. В процессе записи и тестирования на заводе гарантируется, что не будет изготовлено двух приборов с одинаковыми серийными номерами.

Таким образом, исключается возможность подделки приборов. Вполне приемлемой при использовании Touch-memory является и цена: она более чем в 4 раза ниже, чем при использовании пластиковых карточек. Приборы Toich Memory представляют собой энергонезависимую статическую память с многократной записью/чтением, которая размещается внутри металлического корпуса. В отличие от обычной памяти с параллельным портом адреса/данных, память приборов Toich Mempry имеет последовательный интерфейс. Данные записываются/читаются в память по одной двунаправленной сигнальной линии. По этой линии в прибор передаются команды и данные, считываются данные. При этом используется широтно-импульсный метод кодирования. Логические сигналы "1" и "0" с уровнем от +5В до ОВ передаются импульсами различной длительности. Такой цифровой интерфейс позволяет подключать приборы Touch Memory непосредственно к персональным ЭВМ или через микропроцессорный контроллер.

Важной особенностью приборов является низкая потребляемая мощность, что позволяет использовать встроенную в корпусе прибора миниатюрную литиевую батарейку для сохранения информации в памяти в течении 10 лет.

Существуют конкретные разработки аппаратно – программных комплексов защиты информации на базе ТМ. В качестве примера рассмотрим систему QPDOS, разработанную специалистами из АО " РНТ ". QPDOS является функциональным расширением MS-DOS и предназначена для использования в составе ПК на базе IBM РС/АТ.

QPDOS полностью контролирует и управляет доступом всех пользователей к ресурсам и данным ПК. В качестве функциональных частей СЗИ QPDOS могут быть включены следующие подсистемы: регистрации и учета, предназначенную для протоколирования событий, происходящих в системе, контроля за возможными попытками НСД, учета сеансов пользователей и генерации отчетов; оперативного контроля, позволяющую оперативно наблюдать с ПК администратора системы за событиями и действиями пользователей, которые происходят на любом ПК в составе сети; контроля целостности и защиты от копирования программного обеспечения; запрещения начальной загрузки с ГМД, предотвращающую возможность обхода системы защиты нарушителем с помощью загрузки ПК со своей системной дискеты; криптографическую, которая представляет собой драйвер MS-DOS, осуществляющий зашифрование и расшифрование информации на отдельных логических дисках ПК в прозрачном для прикладных программ режиме.

Кроме этого подсистема включает средства для генерации ключей шифрования и перешифрования информации на новом ключе, и ввода ключей шифрования в систему с электронных ключей Touch Memory. Система криптографической защиты может использоваться как в чисто программном варианте, так и с аппаратной поддержкой в виде криптоплаты "Криптон - 3", что повышает производительность системы.

Следует отметить, что меры компьютерной безопасности не ограничиваются только средствами защиты, расположенными в самом компьютере - внутри компьютера, или в виде внешних устройств. Все перечисленные выше программные и аппаратно-программные средства защиты информации становятся эффективными лишь при строгом соблюдении целого ряда административных и организационных мер.

Прежде чем строить систему защиты, необходимо оценить затраты на ее создание и возможные затраты на ликвидацию последствий в случае потери защищаемых данных. Защита будет экономически целесообразна только в том случае, если затраты на ее создание будут меньше возможных потерь.

# Заключение.

Проблемы обеспечения сохранности значительно усложняются при организации машинной обработки информации в условиях коллективного пользования, где сосредотачивается, обрабатывается и накапливается информация различного назначения и принадлежности.

Не существует каких-либо причин, по которым в системах машинной обработки данных, базирующихся на современных средствах вычислительной техники, невозможно было бы обеспечить большую степень сохранности данных, чем в обычных системах сбора, накопления и обработки информации. Система должна защищать своих пользователей друг от друга как от случайных, так и целенаправленных угроз нарушения сохранности информации. Кроме того, принятые механизмы обеспечения сохранности должны предоставлять пользователю средства для защиты его программ и данных от него самого.

Совершенствование технологии обработки информации привело к созданию информационных баз данных, содержащих большие объемы разнообразной информации, что тоже предъявляет дополнительные требования к обеспечению сохранности информации.

В системах коллективного пользования, имеющих развитую сеть терминалов, основная сложность обеспечения безопасности состоит в том, что потенциальный нарушитель является полноправным абонентом системы.

Поэтому под термином "защита" подразумевается способ обеспечения безопасности в СОД. Защита информации обычно сводится к выбору средств контроля за выполнением программ, имеющих доступ к информации, хранимой в системе обработки данных (СОД).

# Список литературы:

1. Гайкович В, Першин А. Безопасность электронных банковских систем. - М.,1999.
2. Груздев С. "16 вариантов русской защиты" /КомпьютерПресс №392
3. Груздев С. Электронные ключи. - М. 1993.
4. Карасик И. Программные и аппаратные средства защиты информации для персональных компьютеров / /КомпьютерПресс №3, 1995
5. Мафтик С. Механизмы защиты в сетях ЭВМ. /пер. с англ. М.: МИР, 1993.
6. Петров В.А., Пискарев С.А., Шеин А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах. - М., 1998.
7. Спесивцев А.В. и др. Защита информации в персональных ЭВМ. - М.: Радио и связь, 1993.