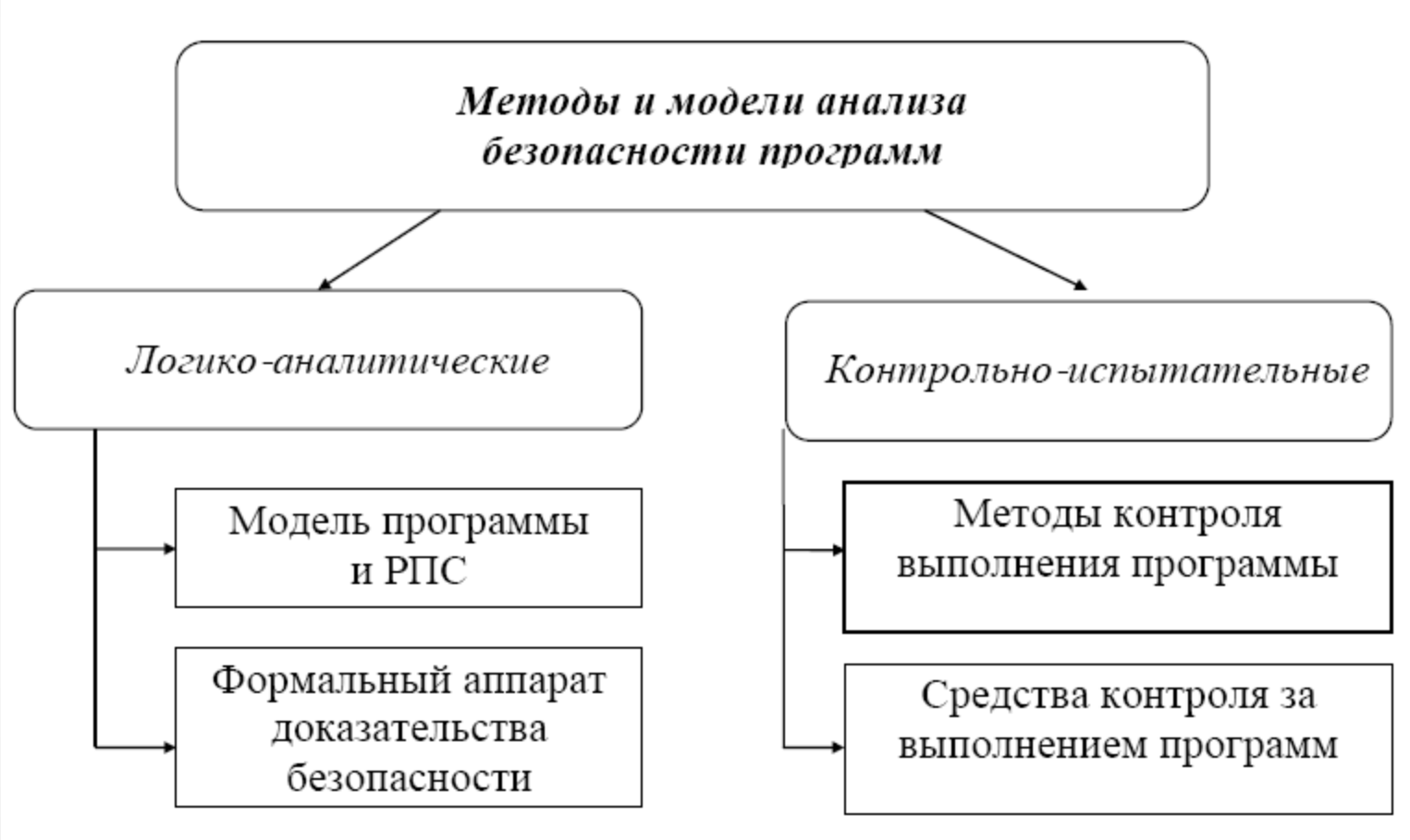
Тема 4

Методы и средства анализа безопасности программного обеспечения

Содержание темы

- Методы и средства анализа безопасности программного обеспечения.
- Методы защиты программного обеспечения.
- Категории средств защиты программного обеспечения.
- Защита программного обеспечения от несанкционированного доступа.
- Защита программного обеспечения от несанкционированного копирования.

Методы и средства анализа безопасности ПО



Методы и средства анализа безопасности ПО

Методы и средства анализа безопасности ПО

Контрольно-испытательные методы - это методы, в которых критерием безопасности программы служит факт регистрации в ходе тестирования программы нарушения требований по безопасности, предъявляемых в системе предполагаемого применения исследуемой программы.

Тестирование может проводиться с помощью тестовых запусков, исполнения в виртуальной программной среде, с помощью символического выполнения программы, ее интерпретации и другими методами.

Методы и средства анализа безопасности ПО

Контрольно-испытательные методы делятся на те, в которых **контролируется процесс выполнения программы** и те, в которых **отслеживаются изменения в операционной среде**, к которым приводит запуск программы.

Последние наиболее распространены, так как они не требуют формального анализа и позволяют использовать имеющиеся технические и программные средства и быстро ведут к созданию готовых методик (*методика пробного запуска в специальной среде с фиксацией попыток нарушения защиты и процедур разграничения доступа*).

Методы и средства анализа безопасности ПО

Схема анализа безопасности программы контрольно-испытательным методом

Методы и средства анализа безопасности ПО

При проведении анализа безопасности с помощью **логико-аналитических методов** строится модель программы и формально доказывается эквивалентность модели исследуемой программы и модели разрушающих программных средств (РПС).

В простейшем случае в качестве модели программы может выступать ее битовый образ, в качестве моделей вирусов множество их сигнатур, а доказательство эквивалентности состоит в поиске сигнатур вирусов в программе.

Более сложные методы используют формальные модели, основанные на совокупности признаков, свойственных той или иной группе РПС.

Методы и средства анализа безопасности ПО

Схема анализа безопасности программы логико-аналитическим методом

Методы и средства анализа безопасности ПО

Полный процесс анализа ПО включает в себя три вида анализа:

- **лексический верификационный** анализ;
- **синтаксический верификационный** анализ;
- **семантический** анализ программ.

Методы и средства анализа безопасности ПО

Лексический верификационный анализ предполагает поиск, распознавание и классификацию различных лексем (сигнатур) программы, представленной в исполняемых кодах.

При этом лексемами являются сигнатуры: **вирусов**, **элементов РПС**, «**подозрительных функций**», **штатных процедур использования системных ресурсов и внешних устройств**.

Поиск сигнатур реализуется с помощью специальных программ-сканеров.

Методы и средства анализа безопасности ПО

Синтаксический верификационный анализ предполагает поиск, распознавание и классификацию синтаксических структур РПС, а также построение структурно-алгоритмической модели самой программы.

Решение задач поиска и распознавания синтаксических структур РПС имеет самостоятельное значение для верификационного анализа программ, поскольку позволяет осуществлять поиск элементов РПС, не имеющих сигнатуры.

Структурно-алгоритмическая модель программы необходима для реализации следующего вида анализа - семантического.

Методы и средства анализа безопасности ПО

Семантический анализ предполагает исследование программы изучения смысла составляющих ее функций (процедур) в аспекте операционной среды компьютерной системы.

В отличие от предыдущих видов анализа, основанных на статическом исследовании, семантический анализ нацелен на изучение динамики программы - ее взаимодействия с окружающей средой.

Методы и средства анализа безопасности ПО

Методы	***Контрольно-испытательные***	***Логико-аналитические***
Способ представления предметной области	Пространство отношений программы с объектами КС.	Пространство программ.
Принцип поиска РПС	Фиксация установления программой нелегитимности отношения доступа к объектам КС.	Доказательство принадлежности программы к множеству РПС.
Поиск проблемы неразрешимости легитимности отношений	С помощью аппроксимации пространства легитимных отношений для данной программы и КС.	С помощью сведения к проблеме разрешимости множества РПС и анализ безопасности относительно разрешимого подмножества РПС.
Решение проблемы перечислимости рабочего пространства	Статистические и экстраполяционные методы теории верификации и функционального тестирования.	Не требуется.

Методы и средства анализа безопасности ПО

Методы	*Контрольно-испытательные*	*Логико-аналитические*
Ошибки первого рода	Весьма вероятны. Чем строже требования, предъявляемые в заданной КС, тем больше вероятность ошибки.	При строгом доказательстве разрешимости подмножества РПС и корректно определенной характеристической функции исключены.
Ошибки второго рода	Маловероятны. Чем строже требования по безопасности, тем меньше вероятность ошибки.	Неизбежны. Определяются мощностью выбранного разрешимого подмножества РПС.

Под ошибкой **первого рода** понимается принятие за РПС безопасной программы, а под **ошибкой второго рода** – объявление программы безопасной, когда на самом деле она содержит РПС.

Методы и средства анализа безопасности ПО

Методы	***Контрольно-испытательные***	***Логико-аналитические***
Преимущества	Не требует теоретической подготовки. Допускает использование имеющихся стандартных программных средств. Устойчивость к ошибкам второго рода. Метод отражает требования конкретных КС.	Опирается на формальные методы. Не требует значительных затрат на этапе применения. Высокая надежность полученных результатов относительно выбранного подмножества РПС. Инвариантность метода по отношению к различным классам программ. Позволяет создавать автоматические простые и доступные средства проверки безопасности.

Методы и средства анализа безопасности ПО

Методы	***Контрольно-испытательные***	***Логико-аналитические***
Недостатки	Проведение испытаний требует существенных затрат времени и других ресурсов. Процесс тестирования требует выделения испытательной КС и должен проводится специалистами.	Подтверждены ошибками второго рода – проверяется лишь часть множества РПС.

Методы защиты ПО

Выделены следующие методы защиты программного обеспечения от несанкционированного использования:

- ✓ методы собственной защиты;
- ✓ методы использования средств защиты в составе вычислительной системы;
- ✓ методы защиты с запросом информации;
- ✓ методы активной защиты;
- ✓ методы пассивной защиты.

Методы защиты ПО

К основным методам **собственной защиты** относятся:

- ✓ методы защиты документации;
- ✓ методы защиты машинного кода;
- ✓ организация сопровождения;
- ✓ ограниченное использование;
- ✓ заказное проектирование;
- ✓ методы защищающие авторское право.

Категории средств защиты ПО

Средства собственной защиты.

Собственная защита программ – это термин, определяющий те элементы защиты, которые присущи самому программному обеспечению и препятствуют незаконным действиям пользователя.

Категории средств защиты ПО

Документация, сопровождающая любое программное обеспечение, является субъектом авторского права и может выполнять функции защиты.

Для этого оригинал документации выполняется в цвете и не может быть качественно воспроизведен одноцветным копировальным устройством, а ее репродуцирование стоит достаточно дорого.

Категории средств защиты ПО

Разработанные программы распространяются, будучи представленными в **машинном коде**, что затрудняет анализ их структуры и обеспечивает определенную степень защиты.

Категории средств защиты ПО

Необходимость **сопровождения** программы со стороны разработчика затрудняет её несанкционированное распространение, особенно в тех случаях, когда программа сложная, требует периодической перенастройки и не полностью отлажена.

Категории средств защиты ПО

Ограниченное применение как способ защиты реализуется в том случае, когда программное обеспечение используется небольшим числом пользователей, каждый из которых известен по имени.

Эта ситуация относительно легко контролируется в окружении, пользующемся доверием, в этом случае условия работы с программными средствами оговариваются в заключаемом контракте

Категории средств защиты ПО

Заказное проектирование предполагает разработку программного обеспечения для специальных целей.

Если программа используется редко, то ее кража в коммерческих целях маловероятна; однако если кража произошла, то именно эти детали дают ключ к источнику несанкционированного копирования

Категории средств защиты ПО

Авторское право – это расстановка отличительных меток в стандартных программных модулях для идентификации программ, поставляемых добросовестным покупателям.

Цена индивидуальной разметки каждой копии программы должна быть тщательно соразмерна с ожидаемой коммерческой прибылью

Методы защиты ПО

К основным методам **использования средств защиты в составе вычислительной системы** относятся:

- ✓ защита магнитных дисков;
- ✓ специальная аппаратура;
- ✓ замки защиты;
- ✓ изменение функций.

Категории средств защиты ПО

Средства защиты в составе вычислительной системы.

Эта категория средств защиты включает защиту дисков и аппаратуры, замки защиты, изменение функций штатных устройств.

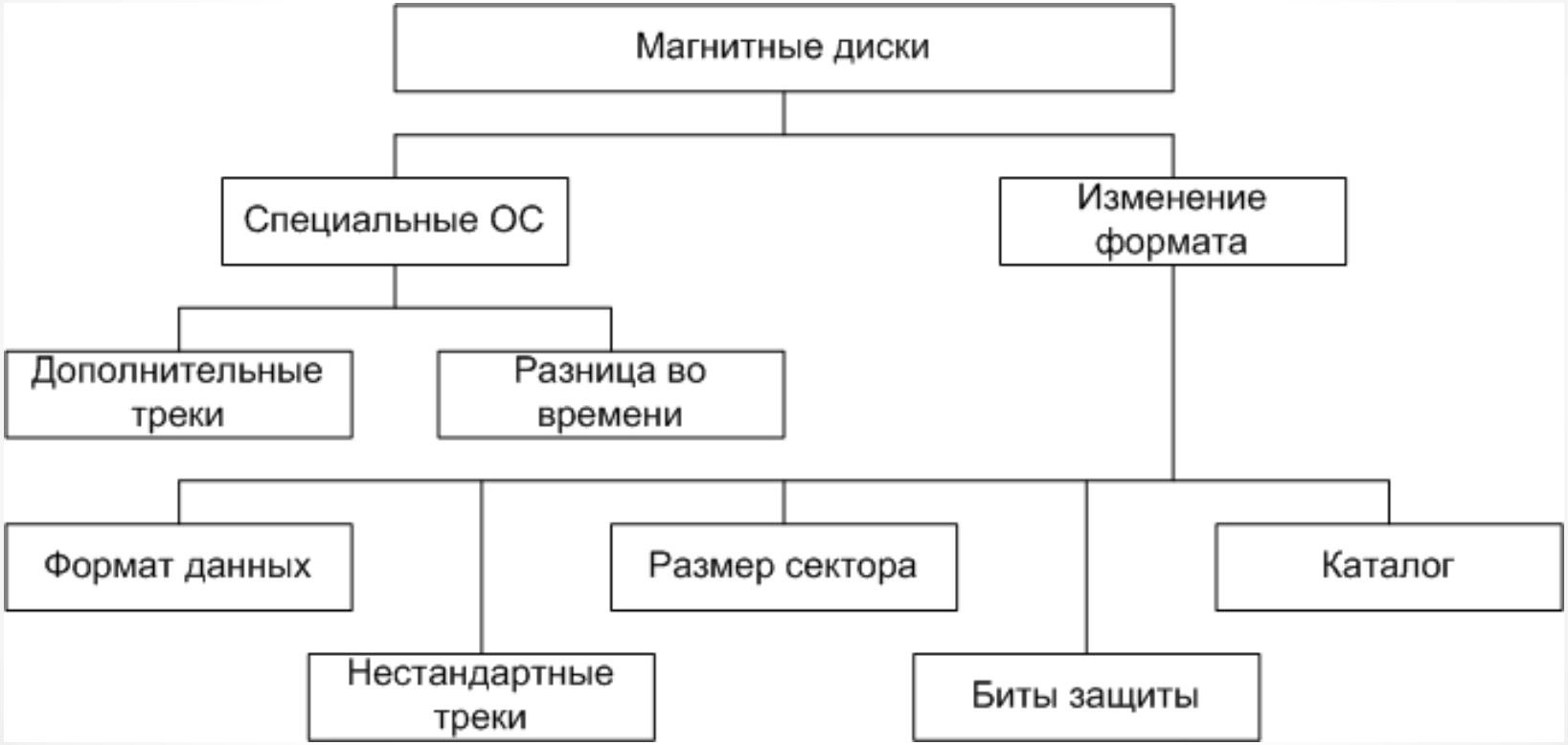
При использовании таких средств операционная среда вычислительной системы в отличие от штатного режима постоянно изменяется, поскольку выполнение программы зависит от определенных действий, специальных мер предосторожности и условий, гарантирующих защиту.

Категории средств защиты ПО

Средства защиты в составе вычислительной системы включают в себя:

- защиту магнитных дисков;
- использование специальной аппаратуры;
- использование замков защиты.

Категории средств защиты ПО



Категории средств защиты ПО

Основная техника защиты дисков заключается в их форматировании специальными способами, которые предохраняют операционную систему от копирования.

Поскольку время обращения к секторам различно, то программным способом можно определить время запаздывания при чтении различных секторов, а поскольку при копировании с помощью стандартной ОС расположение секторов изменится, то запаздывания не будут более соответствовать запаздываниям исходной копии.

Категории средств защиты ПО

Изменение форматов может производиться путём изменения размеров секторов, увеличения числа синхронизирующих битов, заменой информационных заголовков.

Перечисленные методы становятся неэффективными при использовании систем побитового копирования.

Побитовый копировщик – это электронная система копирования, которая осуществляет непосредственное считывание информации, бит за битом.

Категории средств защиты ПО

Для защиты от побитовых копировщиков, используются следующие механизмы:

- биты защиты, которые читаются по-разному в разное время и, таким образом, мешают верификатору копий;
- запись исходной копии со скоростью ниже стандартной, что увеличивает плотность записи, тогда копирование на другой диск со стандартной скоростью вызывает увеличение длины записи и, следовательно, начало дорожки будет испорчено.

Категории средств защиты ПО

Специальная аппаратура.

Использование специальных характеристик аппаратуры для защиты программ является мощным, но дорогостоящим средством.

Перечень возможных вариантов использования специальной аппаратуры включает в себя:

- уникальный диск;
- специальные чипы.

Категории средств защиты ПО

Принцип уникального диска состоит в том, чтобы придать магнитной поверхности диска уникальность, запрещающую запись информации в некоторые секции дорожки.

Это достигается стиранием элементов поверхности с использованием лазерного луча.

Таким образом, требуемый формат каждого диска оказывается уникальным.

Это позволяет, сравнивая скорости чтения разных дисков, различать оригинальный диск от его копии.

Категории средств защиты ПО

Замки защиты.

Замки защиты используются для того, чтобы запретить доступ к программе, если при попытке обращения к ней не выполнены некоторые проверки.

К проверяемым параметрам относятся:

- дата и время использования;
- уникальный серийный номер;
- уникальные дефекты памяти;
- период аренды;
- ресурс работы.

Категории средств защиты ПО

При использовании даты и времени осуществляется контроль предельного времени или даты использования, которые устанавливаются в лицензии, при этом эталоном служат часы компьютера.

Для защиты часов компьютера, т. е. предотвращения несанкционированного доступа к ним, используется либо специальный программный модуль, либо дополнительное оборудование в составе центрального процессора.

Категории средств защиты ПО

Замок, построенный на основе уникального для каждого компьютера серийного номера, относится к классу "мобильных" (настраиваемых, уникальных) замков.

В этом случае программа функционирует только на тех компьютерах, серийные номера которых включены в лицензию.

Возможность доступа к серийному номеру компьютера закладывается в механизм проверки, и программа запускается только после сравнения текущего серийного номера с имеющимся в списке.

Категории средств защиты ПО

Метод, который позволяет придать уникальную характеристику каждому компьютеру, состоит в записи с частичным разрушением памяти.

Блоки динамической памяти в отличие от статической характеризуются тем, что данные в ней должны периодически восстанавливаться путем регенерации.

Данные стираются, если регенерация, связанная с периодической перезаписью, по каким-либо причинам приостанавливается.

Категории средств защиты ПО

Это свойство изменчивости структуры памяти можно использовать в целях идентификации.

Условие функционирования программы можно связать с уникальной структурой памяти.

Запись с частичным разрушением дает уникальный ключ защиты, который предохраняет программу от функционирования на другом компьютере.

Категории средств защиты ПО

Ключи защиты позволяют контролировать использование программного средства в течение заданных интервалов времени с последующим продолжением, т. е. время аренды.

Пользователь выплачивает периодическую (например, ежемесячную) арендную плату и получает на этот срок определенный ключ.

Схема защиты запрещает доступ к программе, если ключ не будет соответствовать показаниям внутренних часов.

Категории средств защиты ПО

Критерием проверки для ключей защиты может служить единица ресурса программного продукта, которой может быть время функционирования программы в секундах или объем данных, извлеченных из базы данных.

В этом методе ключевые слова присваиваются в соответствии с различными номерами устройств, так что пользователь может покупать блоки устройств в соответствии с работой, которая должна быть выполнена.

В дальнейшем длительность использования может быть установлена заново и перезаписана в памяти.

Методы защиты ПО

Методы **защиты с запросом информации** включают в себя:

- ✓ пароли;
- ✓ шифры;
- ✓ сигнатуры;
- ✓ аппаратные средства.

Категории средств защиты ПО

Средства защиты с запросом информации.

Включение механизма защиты в программу связано с разработкой программ с запросом информации, т. е. требующих для своей работы ввода дополнительной информации, такой, как пароли, номера ключей и т. п.

Категории средств защиты ПО

Пароли.

В данном применении пароль является ключом, позволяющим запуск программы.

Каждое программное средство снабжается собственным паролем и, таким образом, любой пользователь, знающий пароль, может его эксплуатировать.

Пароли обеспечивают защиту от несанкционированного использования программного обеспечения в составе вычислительной системы, но для поддержания системы паролей требуется реализация определённой системы требований и условий

Категории средств защиты ПО

Шифры.

Использование шифрования является более сильным методом защиты ПО чем использование паролей.

В исходном состоянии исполнимый код программы или его отдельные части зашифрованы и недоступны для анализа.

В процессе запуска программы требуется ввести ключ, который используется для расшифрования кода целиком или по частям по мере выполнения программы.

Стойкость защиты ПО в этом случае зависит от качества алгоритма шифрования, длины ключа и способа применения шифра.

Категории средств защиты ПО

Так как длинный ключ трудно запомнить в качестве ключа часто используется пароль, преобразованный специальным способом.

Выбор используемого шифра зависит от коммерческих факторов, таких, как стоимость реализации и возможный ущерб от пиратства.

Стремясь уменьшить длину ключа, следует помнить, что от этого зависит степень защиты, которая может оказаться неэффективной при неправильном выборе.

Категории средств защиты ПО

Сигнатуры.

Сигнатура – уникальная характеристика компьютера или других устройств системы, которая может быть использована для защиты и проверена программным способом.

Уникальность гибких дисков проявляется прежде всего в форматировании. Уникальное форматирование позволяет закрепить за таким диском каталог файлов, требуемых для данной программы, чтобы установить нужную вычислительную среду.

Категории средств защиты ПО

К другим возможным сигнатурам относятся длина незаписанных участков магнитной ленты, неиспользованные дорожки на дискете и т. п.

Техника частичного разрушения диска является примером, где сигнатура определяется уникальными характеристиками блока памяти компьютера.

Категории средств защиты ПО

В общем случае в данном методе используются такие характеристики аппаратуры или системы, которые не подвержены изменениям и сами не влияют на нормальное функционирование программного обеспечения.

Если характеристики уникальны для данной вычислительной системы, нормальное прохождение программы может быть выполнено только на ней.

Категории средств защиты ПО

Аппаратура защиты.

Для защиты программного обеспечения аппаратными средствами с запросом информации используются:

- ПЗУ;
- преобразователи информации;
- электронные устройства защиты (ЭУЗ);
- электронные ключи (ЭК).

Категории средств защиты ПО

Принцип защиты программ с использованием ПЗУ состоит в том, что при несанкционированном копировании программы из ПЗУ в оперативную память вырабатывается сигнал на самоуничтожение программы.

В этом случае часть программного обеспечения размещается в ПЗУ и процесс его копирования контролируется операционной системой.

Категории средств защиты ПО

Преобразователи информации, используют некоторые особенности преобразования данных.

В одной из возможных реализаций преобразователя используется микропроцессор, генерирующий в соответствии с алгоритмом псевдослучайное число при нажатии некоторой клавиши клавиатуры.

Если на вычислительной установке имеется такой же алгоритм, оператору достаточно задать правильное число, чтобы подтвердить требуемую последовательность.

Категории средств защиты ПО

Электронные устройства защиты обычно подсоединяются через один их стандартных интерфейсов и откликаются на запрос в виде некоторого числа или последовательности чисел.

Недостаток этого устройства связан с тем, что необходимо управлять доступом к нему из программы, и поэтому хакер может предусмотреть обход такого запроса.

Категории средств защиты ПО

Для предотвращения таких попыток вторжения необходимо повторять запрос на доступ несколько раз и случайным образом.

Кроме того, подлинность исходной программы должна подтверждаться в случайные моменты времени и предусматривать самоуничтожение программы при обнаружении обходов.

Категории средств защиты ПО

Устройства защиты с элементами интеллекта представляют собой одну из форм ЭУЗ со встроенным микропроцессором для реализации сложных алгоритмов защиты.

Такие устройства подсоединяются на параллельный порт компьютера и называются электронными ключами.

Категории средств защиты ПО

Для защиты ПО от пиратства в пользовательское приложение с помощью ЭК внедряется некоторая последовательность блокировок.

Каждая блокировка представляет собой вызов подпрограммы из библиотеки ЭК, для корректного выполнения которой необходимо наличие соответствующего аппаратного ЭК.

При отсутствии ЭК в выполняемую программу возвращается код ошибки, вызывающий завершение исполнения нелегальной копии.

Категории средств защиты ПО

Для защиты от взлома используется несколько методов программирования блокировок:

- частые посылки запросов;
- рассеивание компонентов блокировок;
- использование возвращенных значений в качестве переменных;
- использование контрольных сумм;
- шифрование участков кода.

Категории средств защиты ПО

Один из основных приемов, используемых для запутывания хакеров, состоит в выполнении частых вызовов ЭК, разбросанных по всему коду приложения.

Так как разбрасывание осуществляется случайным образом, то предугадать появление следующей блокировки на большом объёме ПО является затруднительным.

Категории средств защиты ПО

Программные блокировки состоят из нескольких компонентов: запросов ЭК, определения отклика и действий, основанных на результатах подобных определений.

Метод рассеяния заключается в том, что эти компоненты разделяются некоторым количеством кода.

В этом случае устранение программной блокировки, чьи компоненты рассеяны по всему коду, представляет собой очень трудоемкий процесс.

Категории средств защиты ПО

Эффективным приемом является маскировка программных блокировок.

В этом случае значение, возвращенное ЭК становится логическим указателем или ключом выбора следующего шага выполнения программы или следующей подпрограммы.

Другой способ использования возвращенного значения состоит в прибавлении его к значению переменной таким образом, чтобы сумма составляла требуемое значение переменной.

Если указанная переменная используется и в других частях кода, то этот код становится зависимым от вызова ЭК.

Категории средств защиты ПО

Хорошие результаты дает методика защиты, основанная на вычислении контрольных сумм отдельных частей приложения и настройке результата таким образом, чтобы он соответствовал значению, возвращенному ЭК.

Эффективным считается подсчет контрольных сумм с использованием разных алгоритмов.

Это существенно затруднит процесс модификации любой части кода, так как в этом случае необходимо соблюдать условие корректности обеих контрольных сумм.

Категории средств защиты ПО

Для маскировки критических порций данных или кода программы используется их выборочное шифрование.

Так как в качестве ключей шифрования используются значения, возвращаемые ЭК, то необходимым условием расшифрования кода и выполнения приложения является наличие корректного ЭК.

Операцию шифрования можно усложнить путем использования возвращаемых значений ЭК для расшифрования программ, которые, в свою очередь, расшифровывают основной код, используя для этого совершенно другой ключ и алгоритм

Методы защиты ПО

Методы **активной защиты** делятся на:

- ✓ внутренние;
- ✓ внешние.

Категории средств защиты ПО

Средства активной защиты.

Средствами активной защиты называются такие механизмы, которые реагируют на возможные нарушения, связанные с несанкционированным использованием ПО, и вызывают определенные ответные действия по его предупреждению.

Категории средств защиты ПО

К нарушениям, вызывающим инициализацию средств защиты могут относиться:

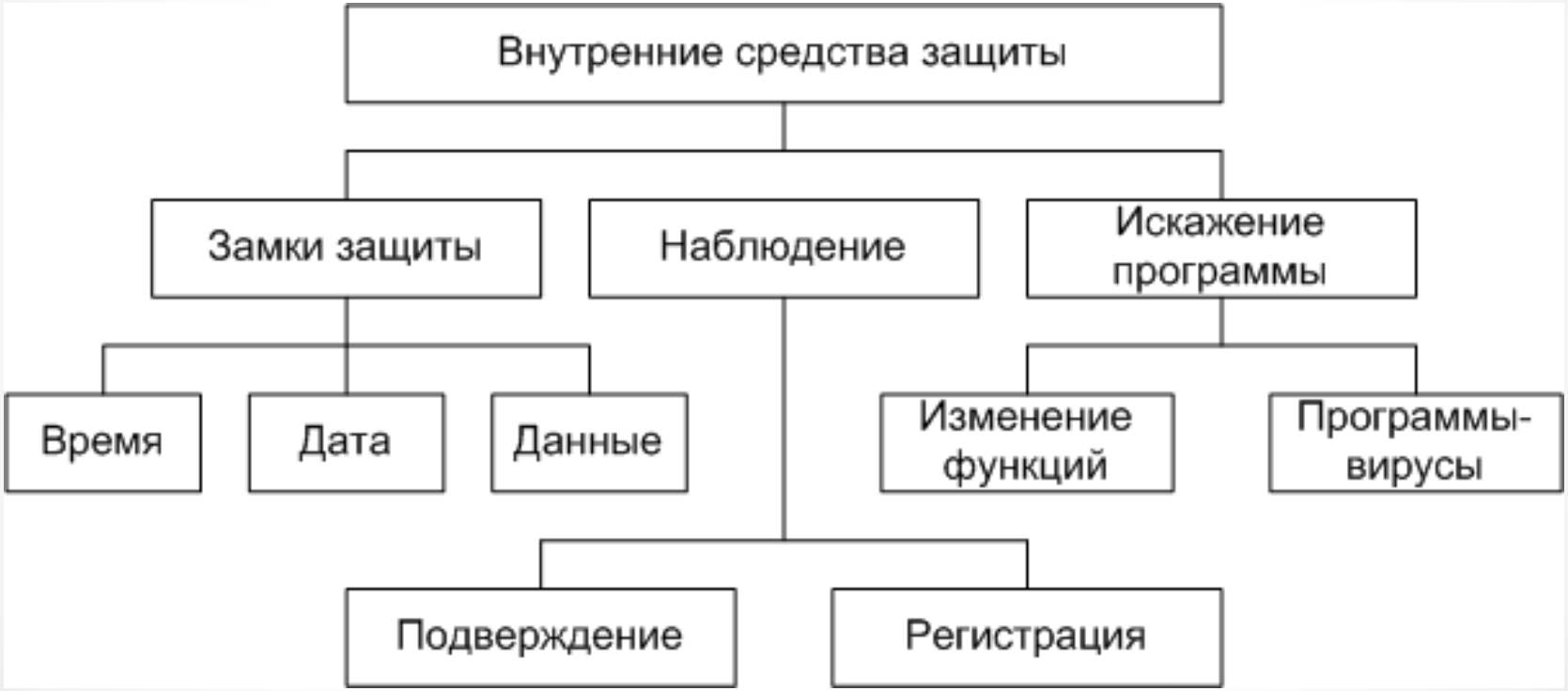
- ввод неправильного пароля;
- указание неправильной даты или времени при запуске программы на выполнение;
- попытки получить доступ к конкретным данным без разрешения на это.

Средства активной защиты делятся на две группы:

- внутренние, используемые для защиты ПО в составе компьютера;
- внешние, используемые для защиты ПО вне его.

Категории средств защиты ПО

Внутренние средства активной защиты



Категории средств защиты ПО

Внутренние средства активной защиты характеризуются тем, что их присутствие в ПО скрывается, пользователям не сообщается об их наличии и возможных последствиях при нарушении условий лицензии. Как правило, внутренние средства защиты либо блокируют программу, либо ее уничтожают.

Категории средств защиты ПО

Замки защиты для блокирования выполнения программы могут быть настроены на любое недозволенное действие, которое будет обнаружено.

Обычно это замки, настроенные на дату, определенное время или на перечень разрешенных ресурсов.

Реакция на несанкционированный доступ может быть реализована в виде блокирования выполнения программы, предупреждения, либо служить поводом для организации наблюдения.

Категории средств защиты ПО

Инициализация наблюдения может начаться с регистрации в системном журнале использования контролируемой программы или реализовываться в виде подтверждения подлинности структуры программы.

Проверкой того, что средства защиты, включенные в программу, не подверглись изменению или удалению.

Категории средств защиты ПО

В качестве реакции на недозволенные действия осуществляется искажение программы путём изменения её функций, или стирание программы в памяти.

Возможен вариант, когда запускается специальная программа-вирус, вызывающая постепенное разрушение программы.

Категории средств защиты ПО

Внешние средства активной защиты

Категории средств защиты ПО

К внешним средствам защиты относятся механизмы, которые в случае возможных нарушений использования ПО, формируют соответствующие сигналы пользователю о незаконности его действий. В группе этих средств общепринятые сигналы тревоги, которые приводят в состояние готовности средства защиты.

Категории средств защиты ПО

Внешние средства включают использование ключевых слов, чтобы вызвать распечатку названия программы или имени ее владельца.

Распечатка авторской этикетки важна, поскольку большинство людей считают, что они действуют законно, и напоминание им о праве собственности владельца вызывает у них некоторую обеспокоенность.

Общепринятые сигналы тревоги используются при создании среды защиты компьютера, когда требуется подтверждение подлинности операции, особенно при копировании.

Методы защиты ПО

Методы **пассивной защиты** делятся на:

- ✓ методы идентификации программ;
- ✓ методы использующие устройства контроля;
- ✓ методы использующие водяные знаки;
- ✓ психологические методы защиты.

Категории средств защиты ПО

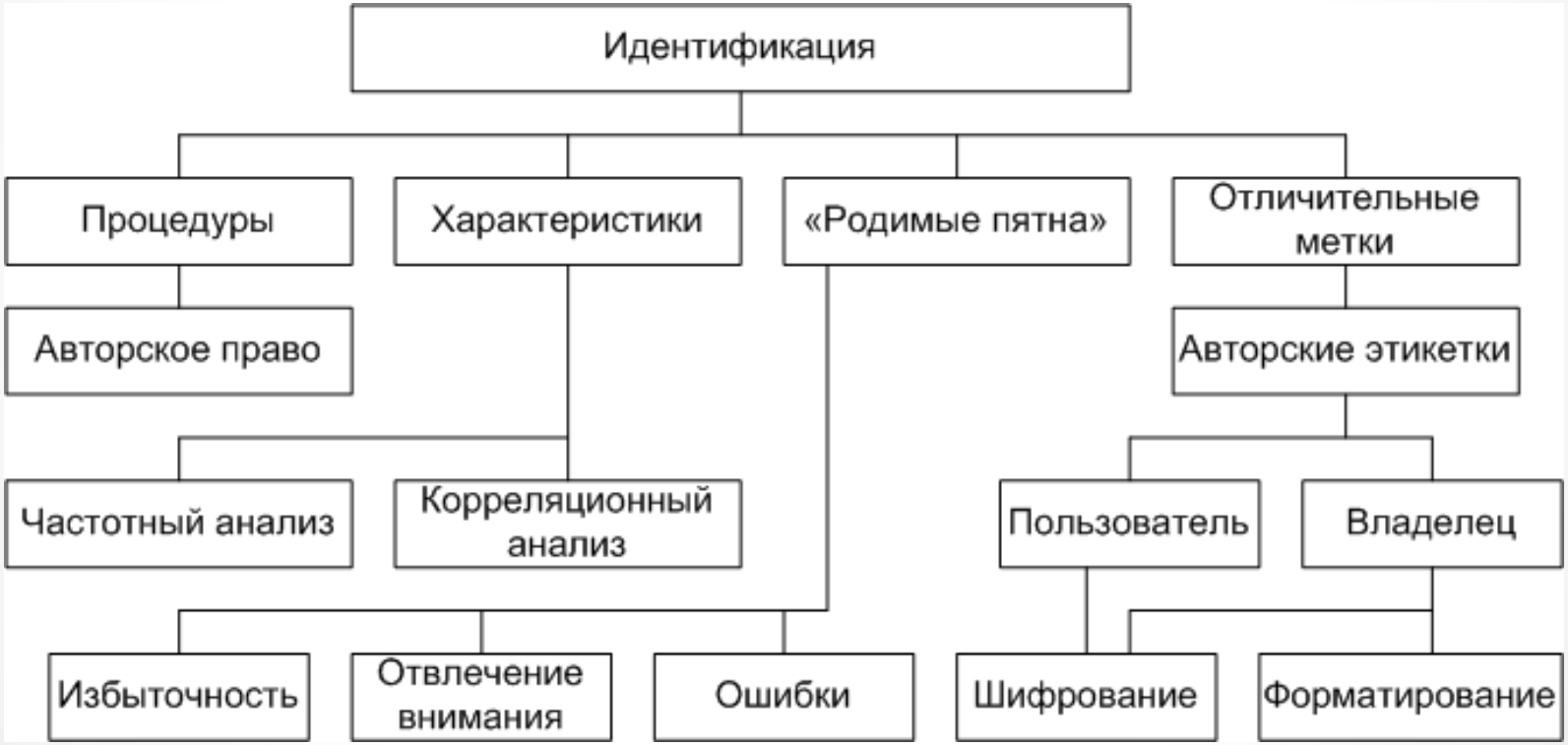
Средства пассивной защиты.

К средствам пассивной защиты относятся:

- идентификация программ;
- контроль программ;
- методы, направленные на поиск улик и доказательство несанкционированного копирования.

Категории средств защиты ПО

Идентификация программ.



Категории средств защиты ПО

Выделение объективных характеристик программы с целью её идентификации – довольно сложная процедура, тем не менее признаки подобия двух программ или модулей, содержащихся в больших программах, определить можно.

Проблема заключается в том, чтобы уметь идентифицировать программы, которые изменены хакером, погружены в другую программу или откомпилированы в машинный код.

Категории средств защиты ПО

Оценка относительной частоты появления операторов или машинных команд – практический способ количественной оценки характеристики программы.

Эта величина изменяется при внесении хакером изменений в программу, однако в большой программе для существенного изменения характеристики требуется выполнить значительную работу.

Категории средств защиты ПО

Для получения корреляционных характеристик, связанных с вставкой программного модуля в большую программу, требуются трудоемкие расчеты, хотя можно указать ряд важных признаков, основанных на частотном или корреляционном анализе, которые указывали бы на сходство исследуемых программ.

Категории средств защиты ПО

Понятие "родимые пятна" используется для описания характеристик, появляющихся в результате естественного процесса разработки программы и относящихся к особенностям стиля программирования, ошибкам и избыточностям, которые не должны иметь места в независимо написанной программе.

Каждое из них может служить убедительной уликой нарушения авторского права.

Категории средств защиты ПО

Отличительные метки, наоборот, относятся к таким признакам, которые не являются случайными, а вводятся специально, чтобы дать информацию об авторе или владельце авторского права.

Другое использование идентификационных меток – выявление путей незаконного копирования или других злоумышленных действий.

Категории средств защиты ПО

Одно из убедительных доказательств копирования – наличие скопированных ошибок.

В каждой программе остаются избыточные части, например подпрограммы, которые были необходимы для отладки в процессе проектирования программного продукта, а затем не были удалены.

В любой программе содержится встроенная улика, которая тем или иным способом сохраняет следы разработки.

Категории средств защиты ПО

Убедительность улики повышается, если отличительная метка, содержащая информацию о владельце авторского права, зашифрована.

Известно много способов включения такой улики, особенно в программы на языках высокого уровня.

Использование зашифрованных отличительных меток – довольно распространенная практика, поскольку при этом они остаются доступными и в машинном коде.

Категории средств защиты ПО

Устройства контроля.

Устройства регистрации событий, процедур или доступа к данным могут рассматриваться как часть общей системы защиты, причем как программ, так и данных.

Подтверждение подлинности программы охватывает проблемы: от установления идентичности функционирования текущей программы и ее оригинала до подтверждения адекватности средств защиты.

Категории средств защиты ПО

Сохранение выполняемой функции наиболее важно при выполнении финансовых сделок, а также для систем автоматизированного проектирования, когда целостность процедуры проектирования не должна быть нарушена. Последнее весьма важно, если используются устройства с низким уровнем защищенности, когда возможен обход проверок, связанных с защитой.

Категории средств защиты ПО

Водяные знаки.

Использование водяных знаков как метода выявления подделки занимает особое место, поскольку препятствует созданию точной копии, которую пользователь не мог бы отличить от оригинала.

Для целей защиты программного кода используются системы цифровых водяных знаков, цель которых – внедрение в код программы методами стеганографии некоторой дополнительной информации, которая не обязательно должна быть секретной.

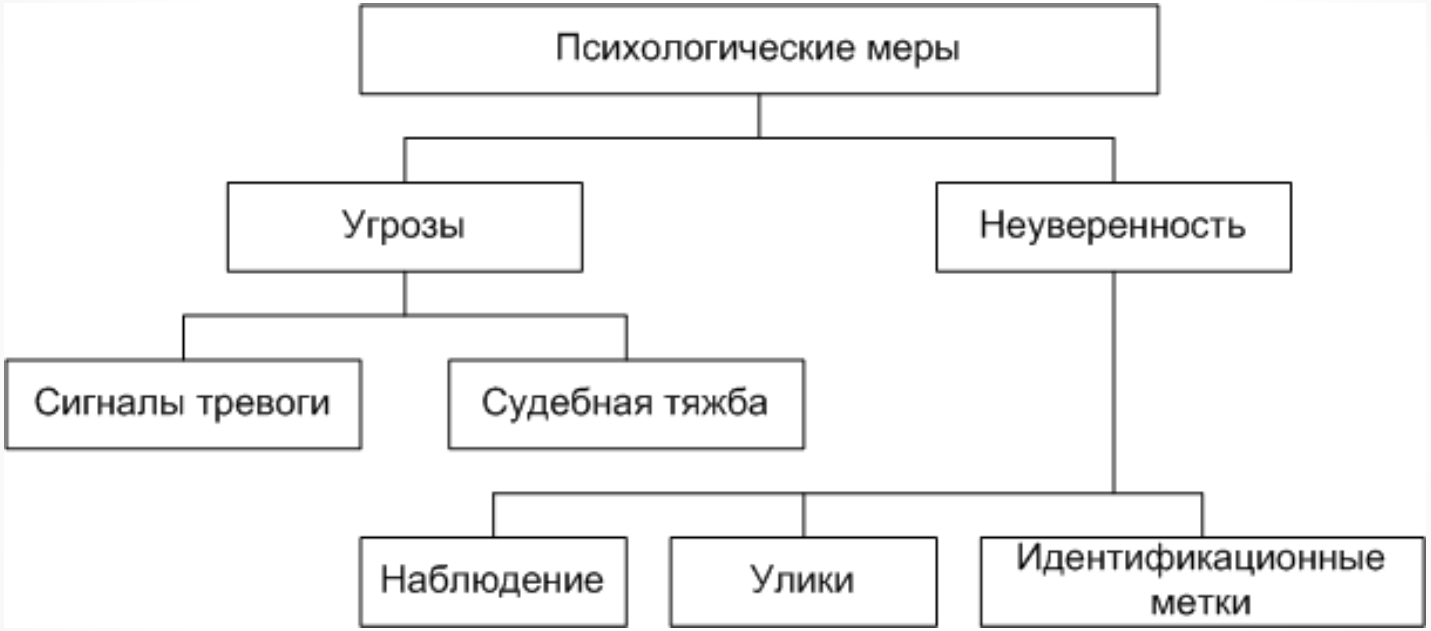
Категории средств защиты ПО

Внедрение производится таким образом, чтобы программный код существенно не искажался, а выделение дополнительной информации оставалось бы возможным после любых преобразований этой дополнительной информации, которые не искажают основной код программы.

Главное свойство ЦВЗ состоит в том, что без знания ключа никто не в состоянии удалить идентификационную информацию, не испортив кода программы.

Категории средств защиты ПО

Психологические методы защиты.



Эти методы основаны на том, чтобы создать у нарушителя чувство неуверенности и психологического напряжения, заставляя его все время помнить, что в похищенном программном продукте могут сохраняться средства защиты.

Методы защиты ПО

Практически каждый метод защиты программного обеспечения использует те или иные средства защиты программного обеспечения, которые объединяются в одноименные с методами категории.

Идеальные методы защиты должны позволять пользователю делать резервные копии для собственного использования и не должны ограничивать возможности компьютера, на который устанавливается защищаемое ПО.

Психологические и социальные факторы должны использоваться в совокупности со средствами защиты и поддерживать в сознании нарушителя обеспокоенность, что будет полезным в дополнение к методам защиты, которые реализованы в ПО.

Защита ПО от НСД

Рассматривая компьютер в составе глобальной или локальной сети как множество компонентов, являющихся объектами нападения, можно выделить три типа несанкционированного доступа (НСД):

- локальный НСД;
- удаленный НСД по сети без доступа непосредственно к компьютеру;
- НСД к информации на отчуждаемых компонентах, т. е. съемных носителях и в канале связи с другими компьютерами.

Защита ПО от НСД

Локальный НСД – попытки получения информации при непосредственном доступе к компьютеру.

Защита ПО от НСД

Для несанкционированного получения информации представляются разумными следующие варианты атак:

1 Атака целевым вирусом (закладкой):

- создать программу-вирус, заражающую программу-драйвер и при вводе пароля сохраняющую пароль в свободных областях на жестком диске;
- внедрить программу-вирус в атакуемый компьютер;
- получить пароли.

Защита ПО от НСД

2 Атака общим вирусом:

- создать программу, которая сохраняет первые несколько десятков байтов ввода после старта программ в скрытом файле;
- внедрить программу-вирус в атакуемый компьютер;
- снять полученную информацию;
- после изучения этой информации выделить пароль в открытом виде.

Против подобных атак можно применить различные проверки целостности программного обеспечения, которые, в свою очередь, могут быть нейтрализованы стелс-механизмами вирусов, и т. д

Защита ПО от НСД

В конце концов можно предложить универсальную закладку, работающую в защищенном режиме микропроцессора, блокирующую всякого рода попытки программ пользователя переключиться в защищенный режим и эмулирующую все известные способы обращения к расширенной памяти.

При таком подходе любые способы контроля целостности ПО не дадут корректного результата.

Гарантированно корректно работает та программа (закладка или средство защиты от нее), которая первой получает управление.

Защита ПО от НСД

Удаленный НСД по сети без доступа непосредственно к компьютеру.

Во многих областях приходится пользоваться импортным программным обеспечением и аппаратными средствами передачи информации по сети с коммутацией пакетов.

Для гарантированной защиты обрабатываемой информации важно, с одной стороны, чтобы управление средствами шифрования не зависело от импортного программного обеспечения, а с другой – чтобы средства защиты были по возможности "прозрачными" по отношению к средствам обработки информации.

Защита ПО от НСД

Использование многих программных продуктов создает дополнительные каналы утечки информации.

Учитывая полное отсутствие на сегодняшний день доверенных отечественных операционных систем и сетевых операционных систем в частности, говорить о передаче по каналам Internet конфиденциальной информации в общем случае не приходится.

Кроме того, свойства семейства протоколов TCP/IP версии 4.0 не позволяют производить гарантированную идентификацию и аутентификацию пользователей.

Защита ПО от НСД

В сложившейся ситуации можно говорить только о передаче конфиденциальной информации по виртуальным сетям.

В данном случае под виртуальной сетью понимается сеть, образованная множеством крипто-маршрутизаторов, использующих Internet как транспортную среду передачи данных.

Защита ПО от НСД

Каждый криптомаршрутизатор защищает свою подсеть посредством шифрования исходящих и расшифровки входящих пакетов.

Криптомаршрутизаторы обмениваются информацией, зашифрованной на ключах парной связи между ними.

Обмен ключами по сети отсутствует.

Защита ПО от НСД

Для закрытия информации эксплуатируется принцип инкапсуляции со скрытием внутренних адресов.

Это означает, что выходящий пакет шифруется полностью вместе с заголовком на ключе парной связи текущего криптомаршрутизатора и криптомаршрутизатора, закрывающего подсеть, содержащую абонента.

Защита ПО от НСД

К этой криптограмме добавляется IP заголовок, с адресом отправителя – внешний адрес текущего криптомаршрутизатора и с адресом получателя – адрес криптомаршрутизатора, закрывающего сеть корреспондента.

Для прохождения полученного пакета через устройства маскировки топологии надсетей (NAT) необходимо к IP заголовку добавить подзаголовок произвольного протокола, например UDP с некоторыми неиспользуемыми портами.

Защита ПО от НСД

Извне обмен информацией между защищаемыми подсетями выглядит как обмен UDP пакетами между парой компьютеров.

Пользователи защищаемых сетей никакого влияния (за исключением некоторого замедления за счет шифрования) не замечают.

Защита ПО от НСД

Все попытки зондирования нарушителем внутренних подсетей будут неудачными, поскольку пришедший пакет не будет правильно расшифрован.

Отсутствие необходимости поддерживать транспортный уровень стека протоколов TCP/IP приводит к недействительности атак на транспортный уровень, что повышает надежность работы криптомаршрутизаторов.

Защита ПО от НСД

НСД к информации на отчуждаемых компонентах, т. е. съемных носителях и в канале связи с другими компьютерами.

Для топологии сети "точка-точка" при возможном внедрении нарушителем произвольных закладок в программное обеспечение компьютеров и работе по коммутируемому или выделенному каналу возможно применение наложенных средств шифрования канала.

Защита ПО от НСД

Если обеспечить включение алгоритмов шифрования в состав каналообразующей, нарушитель:

- не сможет оказывать асинхронное воздействие извне на программно-аппаратные комплексы;
- не получит открытую информацию, передаваемую по каналу при непосредственном съеме информации с линии;
- не получит открытую информацию при перенаправлении ее по коммутируемому каналу.