Параметр	Характеристика абонента				
	магнитная карточка	отпечаток пальцев	отпечаток ладони	голос	подпись
Удобство в пользовании	Хорошее	Среднее	Среднее	Отличное	Хорошее
Идентификация нарушения	Средняя	Отличная	Хорошая	Хорошая	Отличная
Идентификация законности абонента	Хорошая	Средняя	Отличная	Отличная	Хорошая
Стоимость одного устройства, дол.	100	9000	3000	5000	1000
Время распознавания, с	5	10	5	20	5
Надежность	Хорошая	Средняя	Отличная	Хорошая	Хорошая

- **Средства обеспечения информационной безопасности можно условно разделить на следующие группы:**
- **системы контроля доступа** (управляют правами доступа пользователей, регистрируют обращения к защищаемым данным, осуществляют аутентификацию пользователей и сетевых систем (установление подлинности имени объекта для получения им права использования программ и данных));
- **системы шифрования информации** (кодируют данные, хранящиеся на локальных дисках пользователей и передаваемые по телекоммуникационным каналам);
- **системы электронно-цифровой подписи** (обеспечивают аутентификацию получаемой информации и контроль ее целостности);
- **системы антивирусной защиты** (предотвращают заражение файлов на локальных и сетевых дисках, а также распространение вирусов по сети);
- **системы защиты firewall** (осуществляют авторизацию входящего и исходящего трафика между локальной компьютерной сетью и Internet);
- системы резервного хранения и восстановления информации (обеспечивают запись информации на резервные носители и, в случае необходимости, ее восстановление на жестких дисках компьютеров предприятия).

Построение модели систем защиты от угроз нарушения целостности

***Целостность информации* - существование информации в неискаженном виде** (неизменном по отношению к некоторому фиксированному ее состоянию).

Важно обеспечение более широкого свойства-достоверности информации, которое **складывается из адекватности *(полноты и точности)*** отображения состояния предметной области **и** непосредственно **целостности** информации, **т.е. ее неискаженности.**

- 1. **Угрозы нарушения конфиденциальности** информации, в результате реализации которых информация становится доступной субъекту, не располагающему полномочиями для ознакомления с ней.
- 2. **Угрозы нарушения целостности** информации, к которым относится любое злонамеренное искажение информации, обрабатываемой с использованием АС.
- 3. **Угрозы нарушения доступности** информации, возникающие в тех случаях, когда доступ к некоторому ресурсу АС для легальных пользователей блокируется.

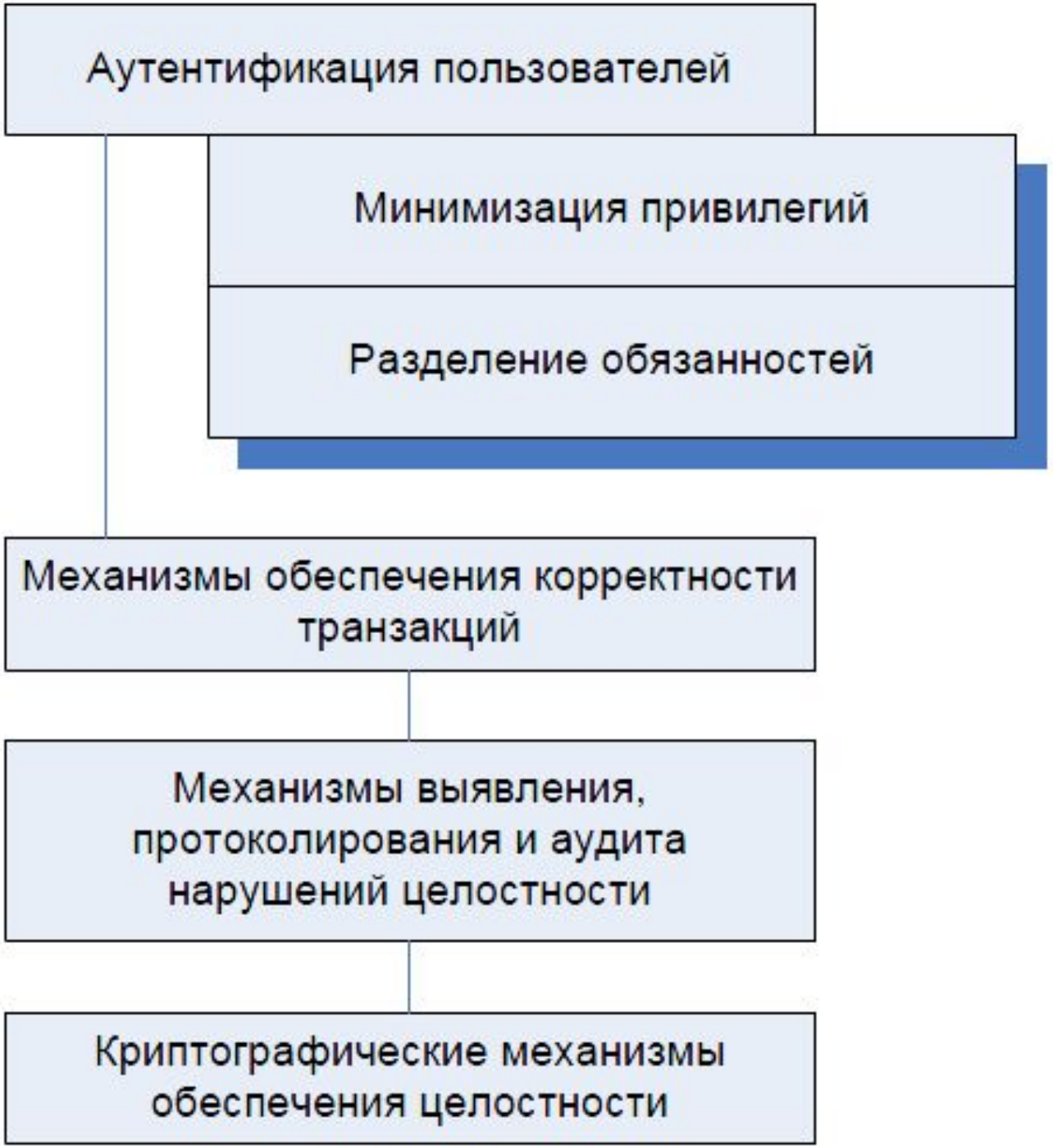
Модель обеспечения конфиденциальности

Рис. 1.3.1. Структура системы защиты от угроз нарушения конфиденциальности информации

- Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения.
- Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью.

ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ

- ***1. Корректность транзакций.*** Невозможность произвольной модификации данных пользователем. Данные должны модифицироваться так, чтобы обеспечивалось сохранение их целостности.
- ***2. Аутентификация пользователей.*** Изменение данных может осуществляться только аутентифицированными пользователями.
- ***3. Минимизация привилегий.*** Пользователи должны быть наделены привилегиями.
- ***4. Разделение обязанностей.*** Для выполнения критических или необратимых операций требуется участие нескольких независимых пользователей.
- ***5. Аудит произошедших событий.*** Данный принцип требует создания механизма подотчётности пользователей, позволяющего отследить моменты нарушения целостности информации.
- ***6. Объективный контроль.*** Необходимо реализовать оперативный контроль.
- ***7. Управление передачей привилегий.*** Порядок передачи привилегий должен полностью соответствовать организационной структуре предприятия.


Аутентификация пользователей
Минимизация привилегий
Разделение обязанностей
Механизмы обеспечения корректности транзакций
Механизмы выявления, протоколирования и аудита нарушений целостности
Криптографические механизмы обеспечения целостности

- **Цифровая подпись представляет собой механизм подтверждения подлинности и целостности цифровых документов.**
- Во многом она является аналогом рукописной подписи – в частности, к ней предъявляются практически аналогичные требования:
- 1. Цифровая подпись должна позволять доказать, что именно **законный автор**, и никто другой, сознательно подписал документ.
- 2. Цифровая подпись должна представлять собой **неотъемлемую часть документа**. Должно быть **невозможно отделить подпись от документа** и использовать её для подписывания других документов.
- 3. Цифровая подпись должна обеспечивать **невозможность изменения** подписанного документа.
- 4. Факт подписывания документа должен быть юридически доказуемым. Должен быть **невозможным отказ от авторства** подписанного документа.

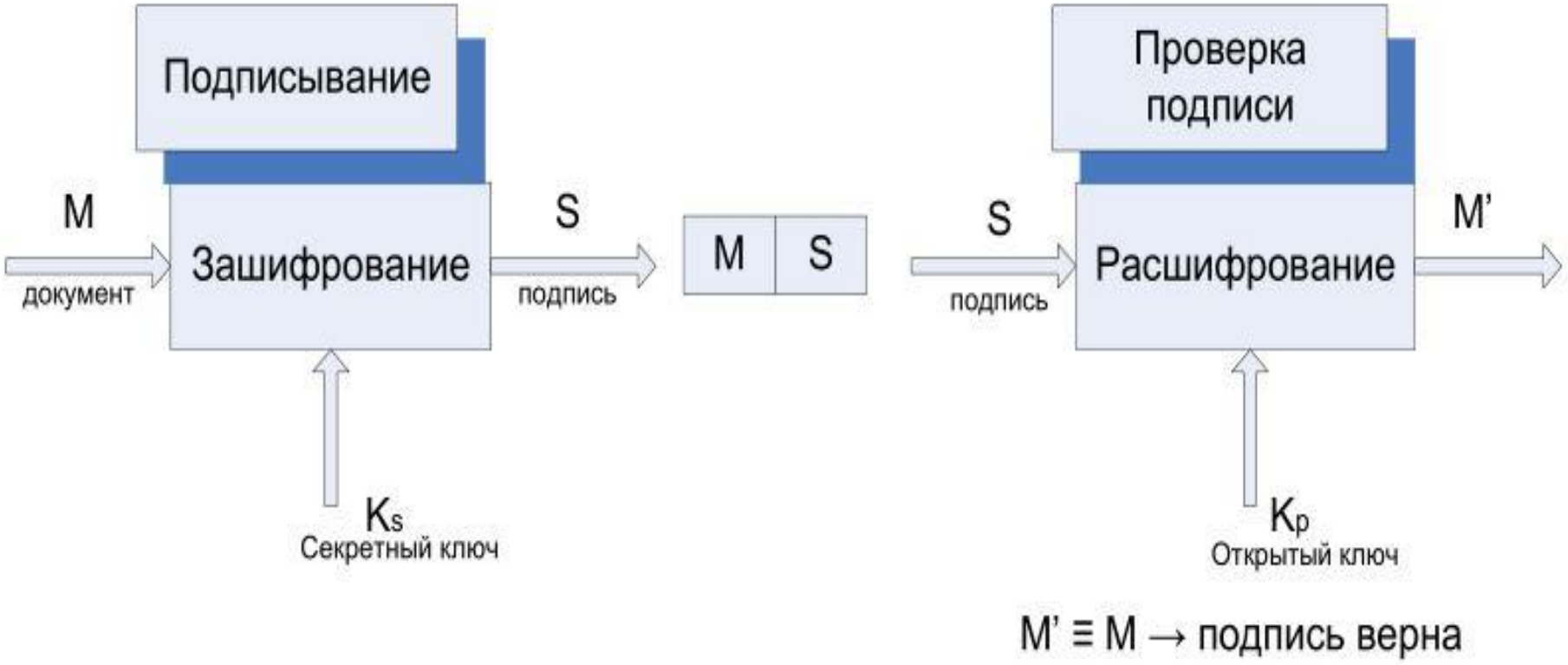


Рис. 1.4.2.1. Реализация механизма цифровой подписи

Рис. 1.5.1. Структура системы защиты от угроз нарушения доступности

- **Резервное копирование информации является одним из важнейших механизмов, обеспечивающих её доступность и целостность.** Используются следующие **методы резервного копирования**:
- 1. **Полное** /full/. В этом случае все без исключения файлы, потенциально подвергаемые резервному копированию, переносятся на резервный носитель.
- 2. **Инкрементальное** /incremental/. Резервному копированию подвергаются только файлы, изменённые с момента последнего инкрементального копирования.
- 3. **Дифференциальное** /differential/. Копируются файлы, изменённые с момента полного резервного копирования. Количество копируемых данных в этом случае с каждым разом возрастает.

- **Зеркалирование серверов** в целом аналогично зеркалированию дисковых накопителей: идентичные данные в целях защиты от сбоев оборудования записываются на два независимых сервера. Речь в данном случае идёт исключительно о хранении данных.
- Дублирование серверов, в свою очередь, позволяет обеспечить полноценную замену сервера в случае его сбоя за счёт передачи управления резервному серверу.
- Механизмы избыточной маршрутизации позволяют за счёт использования избыточных маршрутизаторов и дополнительных соединений гарантировать возможность передачи в случае недоступности части маршрутов.

- Дублирование каналов связи может осуществляться как в пределах автоматизированной системы, так и в отношении каналов, связывающих АС с внешней средой (например, путём использования каналов доступа к Internet от нескольких независимых провайдеров).
- Дублирование шлюзов и межсетевых экранов позволяет избежать ситуации, когда связность АС нарушается из-за неисправности узла, представляющего собой «узкое место» - единую точку входа для всего трафика.

- **Суть VPN** состоит в следующем :
- На все компьютеры, имеющие выход в Internet (вместо Internet может быть и любая другая сеть общего пользования), ставится **средство, реализующее VPN**. Такое средство обычно называют **VPN-агентом**. VPN-агенты обязательно должны быть установлены на все выходы в глобальную сеть.
- VPN-агенты автоматически зашифровывают всю информацию, передаваемую через них в Internet, а также контролируют целостность информации с помощью **имитоприставок**.

- **Перед отправкой IP-пакета VPN-агент выполняет следующее:**
- Анализируется IP-адрес получателя пакета.
- Выбираются алгоритмы защиты данного пакета.
- Вычисляется и добавляется в пакет его имитопристаВка.
- Пакет шифруется.
- **При получении IP-пакета выполняются обратные действия:**
- Из заголовка пакета получается информация о VPN-агенте отправителя пакета.
- Выбираются криптографические алгоритмы и ключи.
- Пакет расшифровывается, затем проверяется его целостность. Пакеты с нарушенной целостностью также отбрасываются.

- VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (к таким каналам обычно применяется термин «туннель», а технология их создания называется «туннелированием»). Вся информация идет по туннелю только в зашифрованном виде.
- Как видно из описания действий VPN-агентов, часть IP-пакетов ими отбрасывается. Действительно, VPN-агенты фильтруют пакеты согласно своим настройкам (совокупность настроек VPN-агента называется «Политикой безопасности»). То есть VPN-агент выполняет два основных действия: создание туннелей и фильтрация пакетов


VPN-агент
VPN-агент
Интернет
Туннель
Фильтр
Фильтр