

Способы обеспечения ИБ в КС

Фрагментарный подход

Отдельные средства
управления доступом

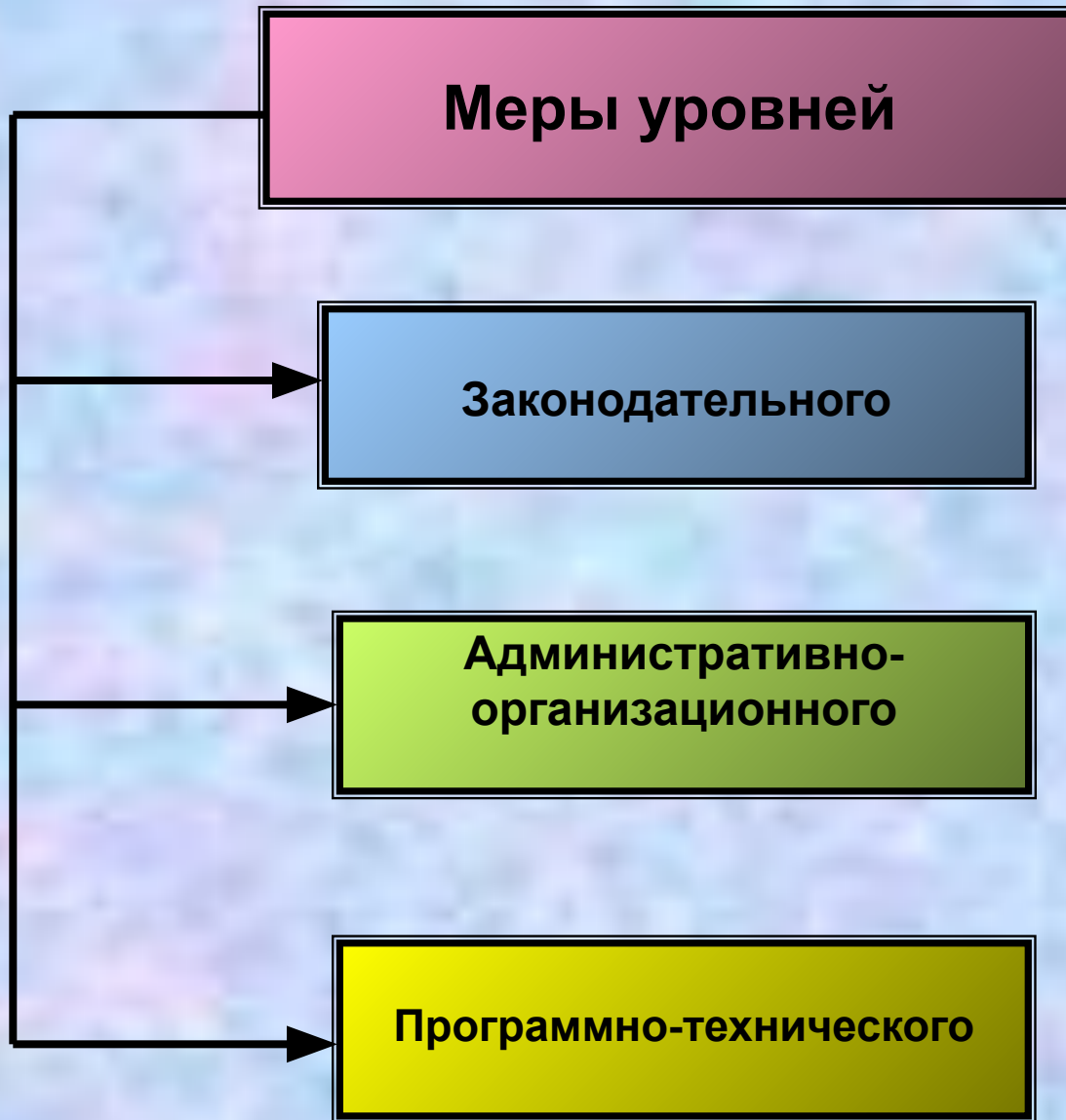
Автономные средства
шифрования

Специализированные
антивирусные
программы

Комплексный подход

Защита КС
крупных предприятий

Защита небольших КС,
выполняющих
ответственные задачи

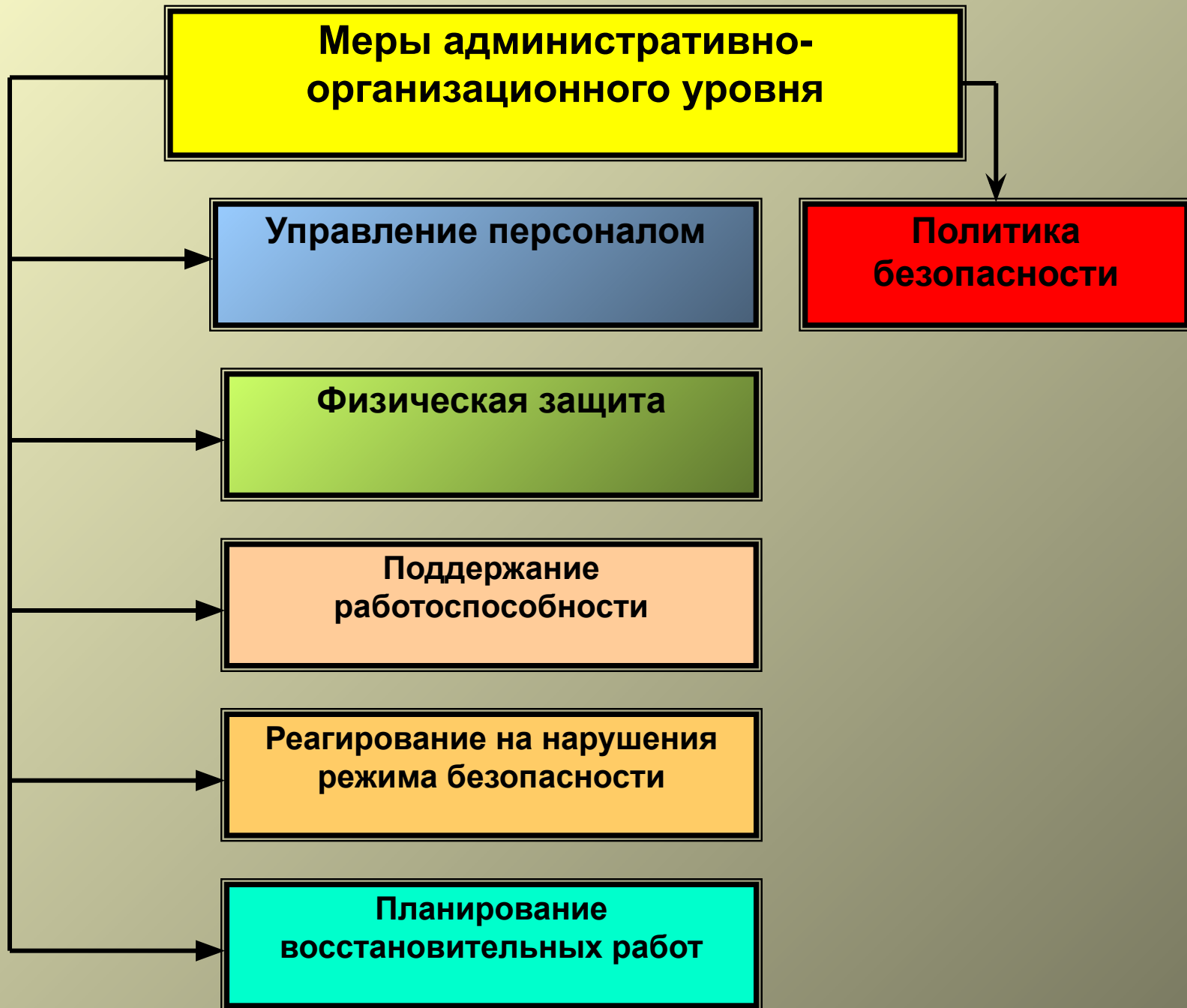


Меры уровней

Законодательного

**Административно-
организационного**

Программно-технического



**Меры административно-
организационного уровня**

Управление персоналом

Физическая защита

**Поддержание
работоспособности**

**Реагирование на нарушения
режима безопасности**

**Планирование
восстановительных работ**

**Политика
безопасности**

Задачи по реализации мер защиты административно-организационного уровня

- **развёртывание системы контроля и разграничения физического доступа к элементам автоматизированной системы;**
- **создание службы охраны и физической безопасности;**
- **организацию механизмов контроля за перемещением сотрудников и посетителей (с использованием систем видеонаблюдения, проксимити-карт и т.д.);**
- **разработку и внедрение регламентов, должностных инструкций и тому подобных регулирующих документов;**
- **регламентацию порядка работы с носителями, содержащими конфиденциальную информацию.**

Стандарты ИБ

Меры и средства программно-технического уровня

Идентификация и аутентификация

Управление доступом

Протоколирование и аудит

Криптография

Экранирование

Обеспечение высокой доступности

Механизмы безопасности

Модель комплексной системы защиты

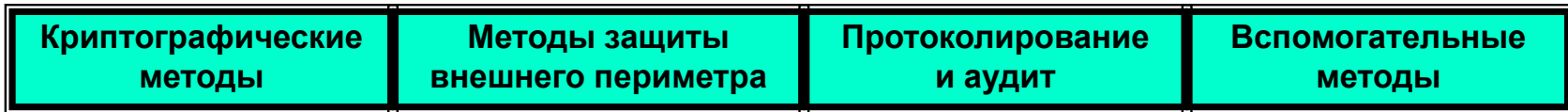
Организационные меры и меры обеспечения физической безопасности



Идентификация и аутентификация



Разграничение доступа



Методы защиты информации от утечки по техническим каналам

Направления обеспечения защиты информации

Аутентификация

Право на частную, персональную информацию

Определение событий безопасности (Security Events)

Защита корпоративного периметра

Определение атак

Контроль за потенциально опасным содержимым

Контроль доступа

Администрирование

Реакция на события (Incident Response)

Механизмы и средства защиты информации

Защищенные коммуникационные протоколы

Средства криптографии

Механизмы аутентификации и авторизации

Средства контроля доступа к рабочим местам сети и из сетей общего пользования

Антивирусные комплексы

Программы обнаружения атак и аудита

Средства централизованного управления контролем доступа пользователей, безопасного обмена пакетами данных и сообщениями любых приложений по открытым IP-сетям

Задача получения злоумышленником доступа к информации

- выбор соответствующего заданному носителю привода – наиболее значимого для обеспечения доступа элемента;**
- запуск соответствующего приводу комплекта программ (операционная система, драйверы привода и т.п.);**
- обеспечение порядка использования программ и привода для считывания в память компьютерной системы содержимого носителя информации**

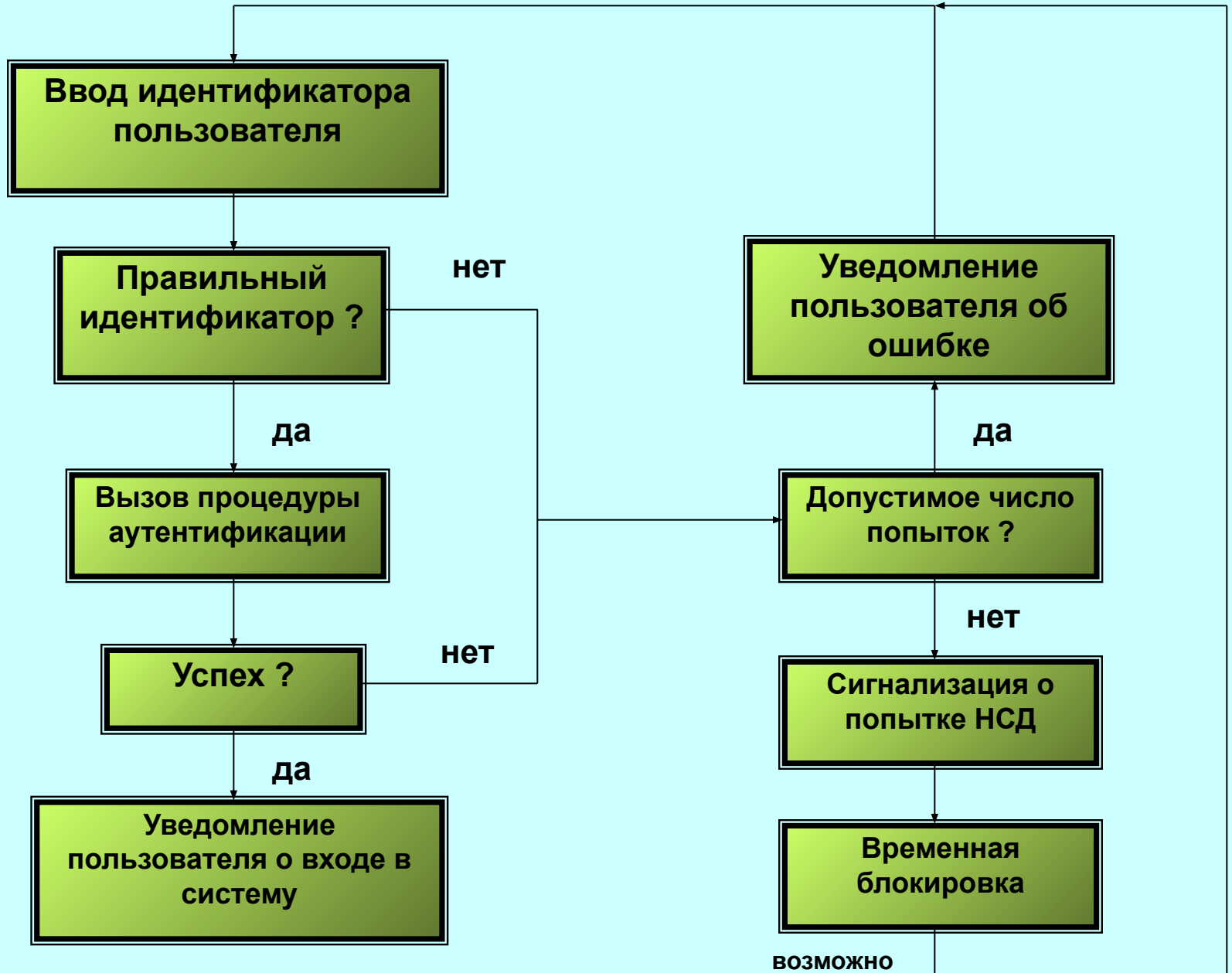
Задачи обеспечения защиты информации в АС на уровне МНИ

- исключение прохода носителей по технологическим участкам, не обусловленным производственной необходимостью**
- предупреждение непосредственного доступа к носителям персонала, не отвечающего за операции с носителями (минимизация доступа), предупреждение утраты или хищения носителей информации**

Регламентация порядка обращения с МНИ

- **Запись информации (создание носителей с информацией) на рабочих местах, обеспечивающих условия для предотвращения утечки по техническим каналам и физической сохранности носителей.**
- **Постановка на учет МНИ с простановкой соответствующей маркировки на зарегистрированном носителе. Одним из элементов маркировки должен быть гриф секретности информации, хранящейся на данном носителе.**
- **Передача МНИ между подразделениями организации, эксплуатирующей АС, под расписку.**
- **Вынос МНИ за пределы организации только с разрешения уполномоченных лиц.**
- **Хранение МНИ в условиях, исключающих несанкционированный доступ посторонних. Для хранения рекомендуется использовать надежно запираемые и опечатываемые шкафы. Надлежащие условия хранения должны быть обеспечены для всех учтенных носителей, независимо от того, находятся ли они в эксплуатации или нет.**
- **Уничтожение МНИ, которые утратили свои эксплуатационные характеристики или не используются из-за перехода на новый тип носителя, специально организованными комиссиями согласно актам, утверждаемым уполномоченными лицами. Уничтожение носителей должно проводиться путем их физического разрушения, не допускающего восстановление и повторное использование носителей. Перед уничтожением конфиденциальная информация должна быть по возможности гарантированно удалена.**
- **Передача в ремонт средств вычислительной техники без МНИ, которые могут содержать конфиденциальную информацию (без накопителей на жестких дисках и т.п.). В случае ремонта МНИ конфиденциальная информация на них должна быть гарантированно удалена. Если удалить информацию невозможно, решение о ремонте принимается руководителем соответствующего подразделения или коллегиально, а ремонт осуществляется в присутствии лица, ответственного за сохранность информации на данном носителе.**
- **Периодический контроль контролируемыми подразделениями соблюдения установленных правил обращения с носителями и их физической сохранности.**

Схема идентификации и аутентификации



Рекомендации по практической реализации парольных систем

- **установление минимальной длины пароля**
- **увеличение мощности алфавита паролей**
- **проверка и отбраковка паролей по словарю**
- **установка максимального срока действия пароля**
- **установка минимального срока действия пароля**
- **отбраковка по журналу истории паролей**
- **ограничение числа попыток ввода пароля**
- **принудительная смена пароля при первом входе пользователя в систему**
- **задержка при вводе неправильного пароля**
- **запрет на выбор пароля пользователем и автоматическая генерация пароля**

Основные параметры парольных систем

A – мощность алфавита паролей;

L – длина пароля;

$S = A^L$ – мощность пространства паролей;

V – скорость подбора паролей;

T – срок действия пароля;

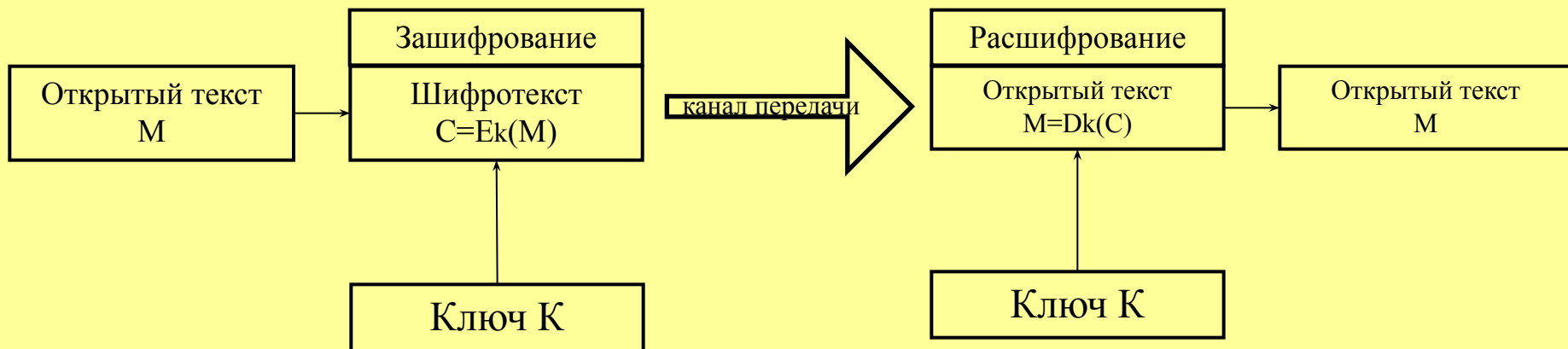
P – вероятность подбора пароля в течение его срока действия.

A – мощность алфавита паролей;
 L – длина пароля;
 $S = A^L$ – мощность пространства паролей;
 V – скорость подбора паролей;
 T – срок действия пароля;
 P – вероятность подбора пароля в течение его срока действия.

Методы хранения и передачи паролей

- **в открытом виде**
- **в виде хэш-значения**
- **в зашифрованном виде**

Структура симметричной криптосистемы



Структура асимметричной криптосистемы

