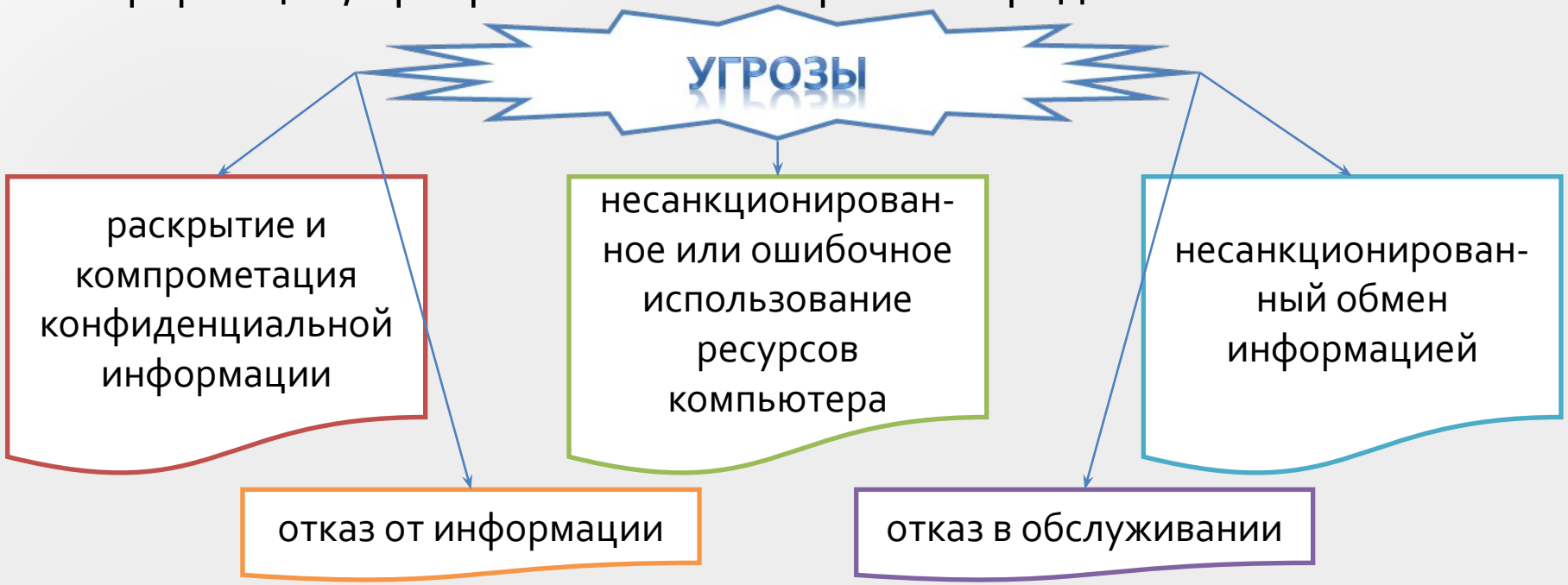
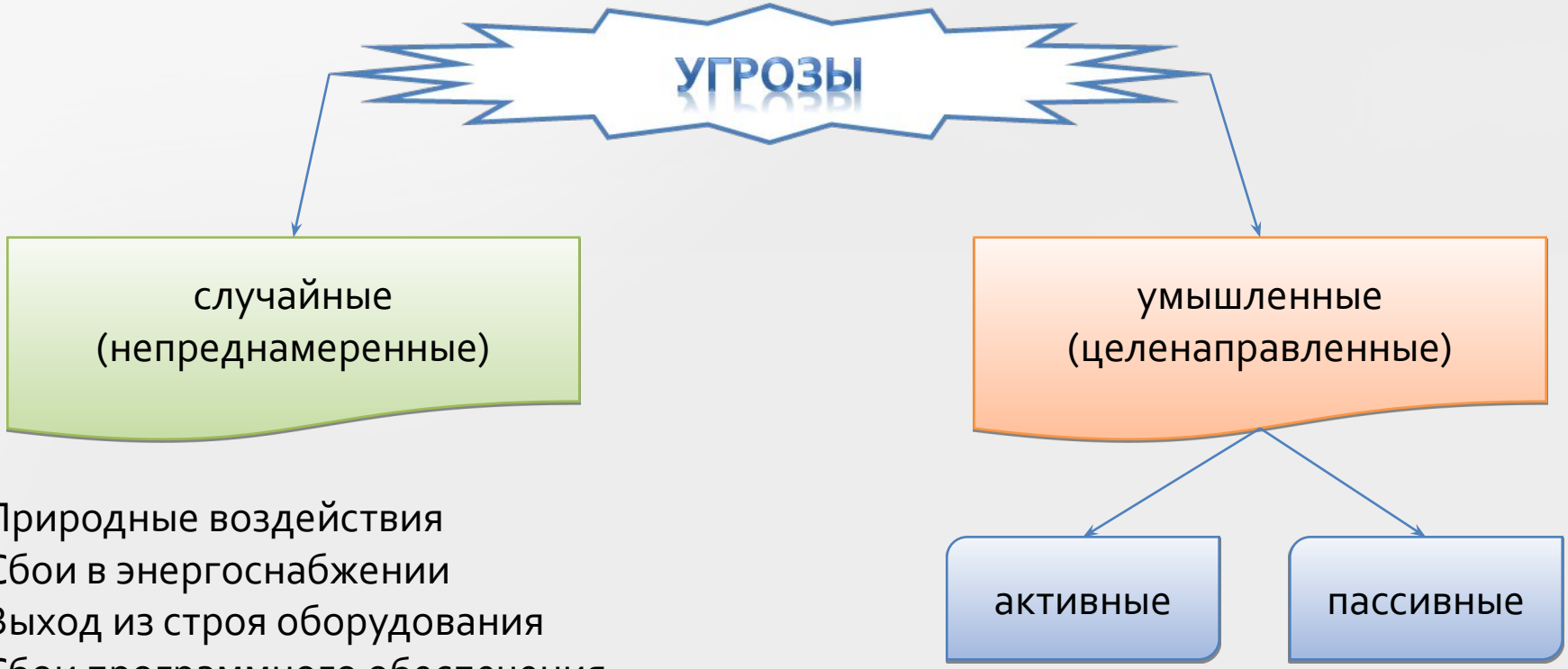
Компьютерная безопасность

Угрозы компьютерной безопасности

Угроза компьютерной безопасности - это действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов компьютера: хранимой, передаваемой и обрабатываемой информации, программных и аппаратных средств.



Угрозы компьютерной безопасности



- Природные воздействия
- Сбои в энергоснабжении
- Выход из строя оборудования
- Сбои программного обеспечения
- Неумелые пользователи

Угрозы компьютерной безопасности

Меры по обеспечению компьютерной безопасности:

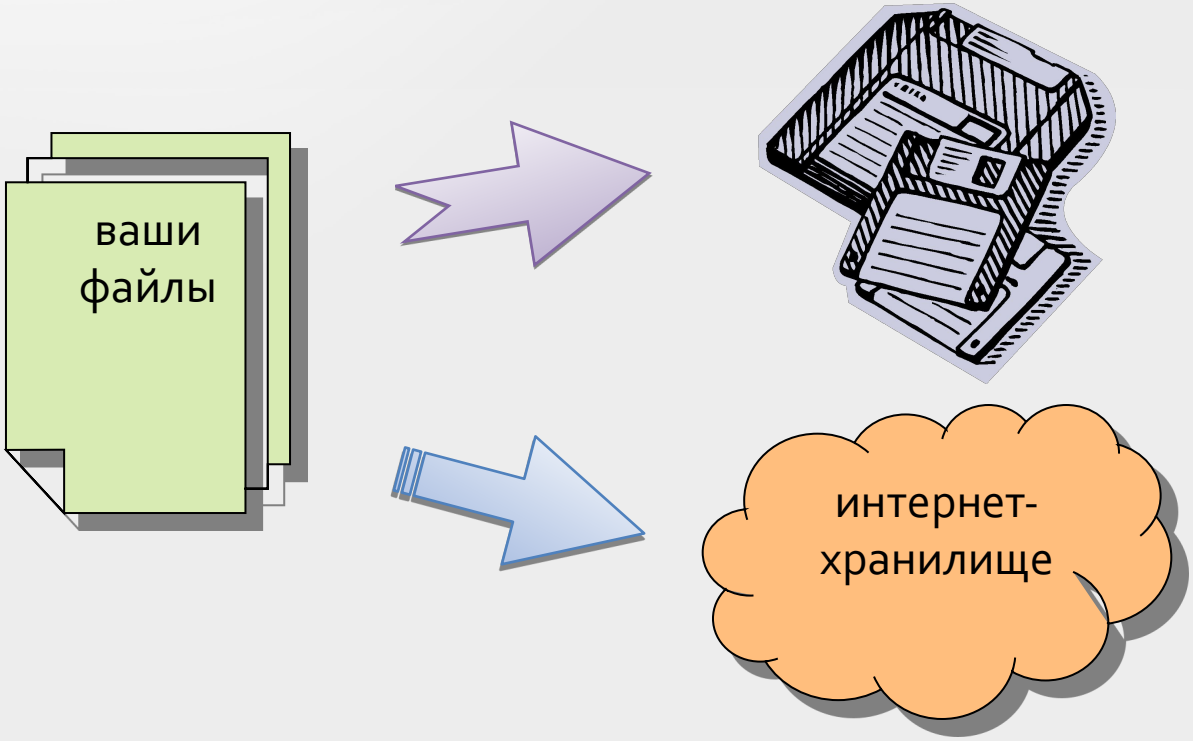
- Обеспечение работоспособности компьютера
- Предотвращение несанкционированного доступа
- Противодействие вредоносным программам

Обеспечение работоспособности

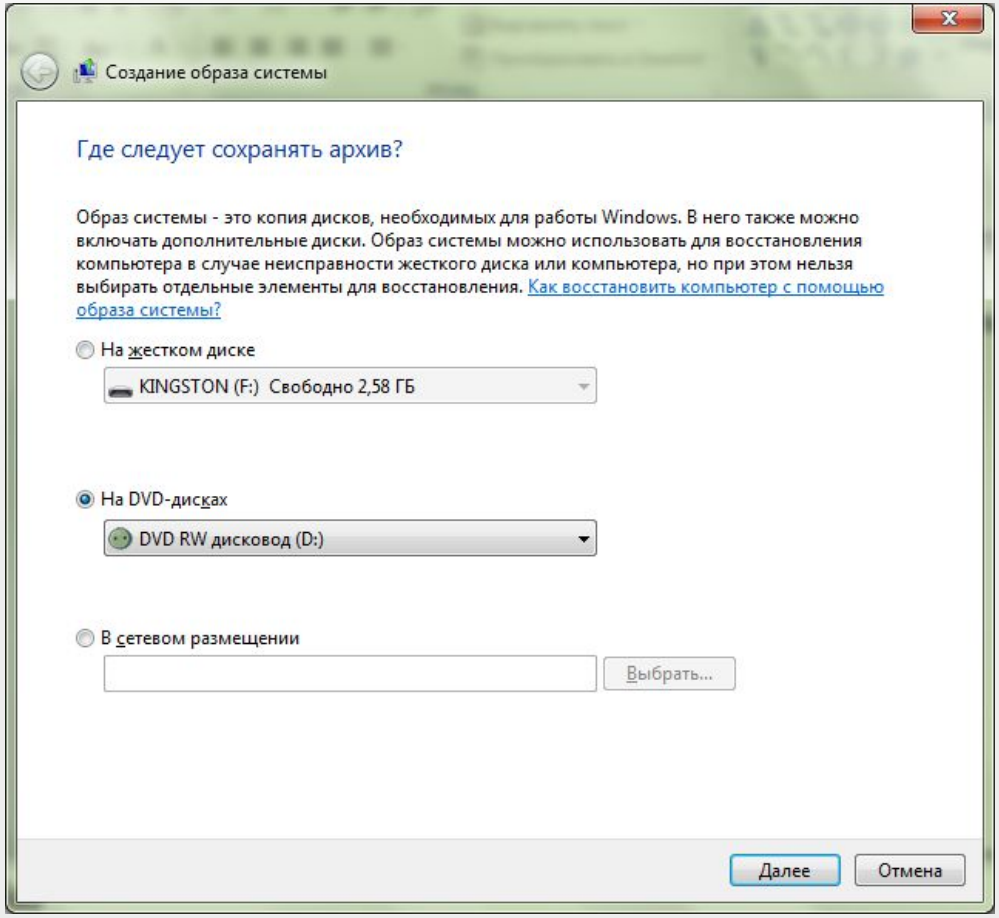
Предотвращение потери информации при случайных сбоях или авариях аппаратуры, повреждениях программ и данных, связанных с ошибками в работе самого пользователя.

Резервное копирование (архивация)

Для обеспечения возможности восстановления данных после аварийных ситуаций необходимо регулярно проводить *резервное копирование данных*.



Программы архивации данных



Защита от чужих

- идентификация и аутентификация;
- разграничение доступа;
- аудит - мониторинг несанкционированных действий;
- криптографические методы защиты данных

Аутентификация

Аутентификация - средство защиты, определяющее подлинность пользователя и законность его работы.

Виды аутентификации:

- Защита паролем
- Смарт-карта, дискета, жетон т.д.
- Отпечаток пальца и другие виды биометрической аутентификации

Разграничение доступа

Доступ - операция, которая может быть осуществлена над объектом.

Разграничение доступа - совокупность правил, определяющая для каждого сочетания субъекта, метода и объекта, наличие или отсутствие у данного субъекта права доступа к данному объекту по данному методу.

Разграничение доступа

Модели разграничения доступа

дискреционная

- каждый объект имеет своего владельца;
- владелец определяет права доступа;
- определена возможность доступа для каждого сочетания субъекта, метода и объекта;
- администратор может обращаться к любому объекту с использованием любого метода доступа.

полномочная (мандатная)

- определен упорядоченный набор грифов секретности;
- для каждого объекта задан гриф секретности;
- для каждого субъекта определен уровень допуска.

Аудит

Одной из составляющих политики безопасности является контроль за функционированием компьютерных систем, при котором происходящие события регистрируются в специальном журнале – *журнале аудита*.

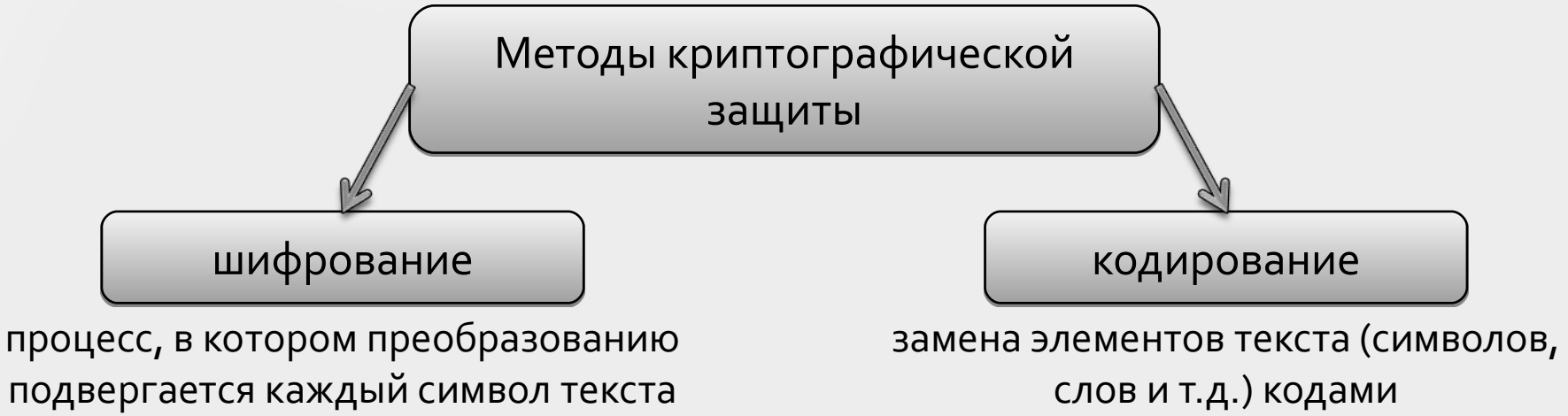
Система аудита должна удовлетворять следующим требованиям:

- формировать записи в журнале аудита может только компьютерная система;
- записи нельзя ни удалять, ни редактировать;
- доступ к журналу имеют только специально назначенные пользователи;
- очищать журнал могут только аудиторы, перед очисткой должна создаваться страховая копия.

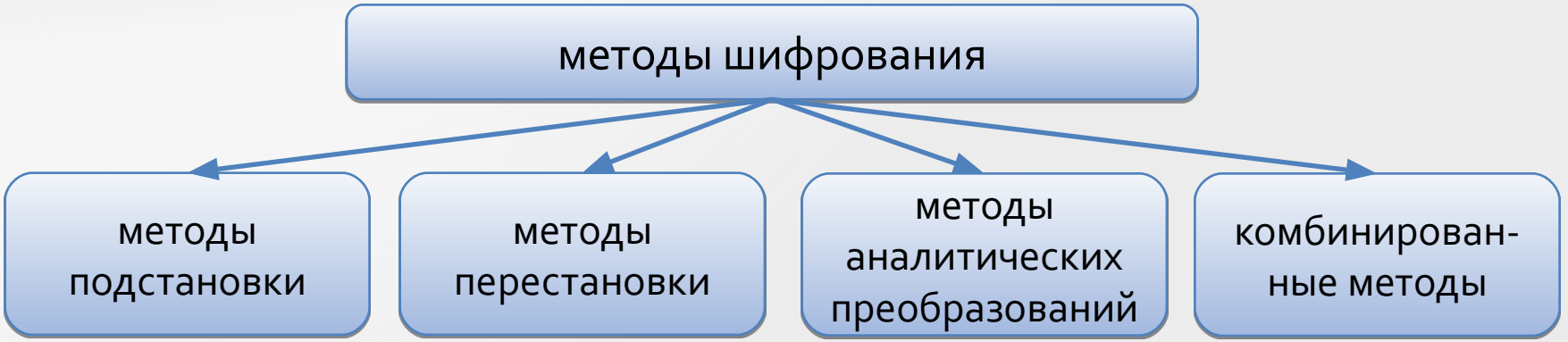
Криптография

Криптография (греч. *kryptos* – тайный и *grapho* – пишу) используется для изменения сообщения с целью сделать его текст непонятным для непосвященных лиц. Процесс преобразования исходных данных в зашифрованные называется шифрованием.

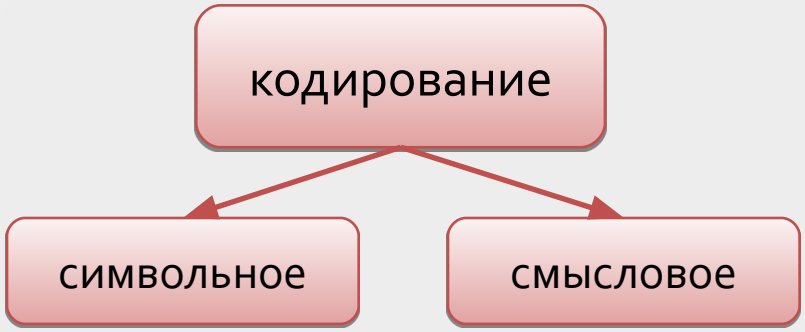
Стойкость – минимальный объём шифротекста, который можно восстановить с помощью статистического анализа, т.е. стойкость шифра определяет объём данных, который можно защитить с его помощью.

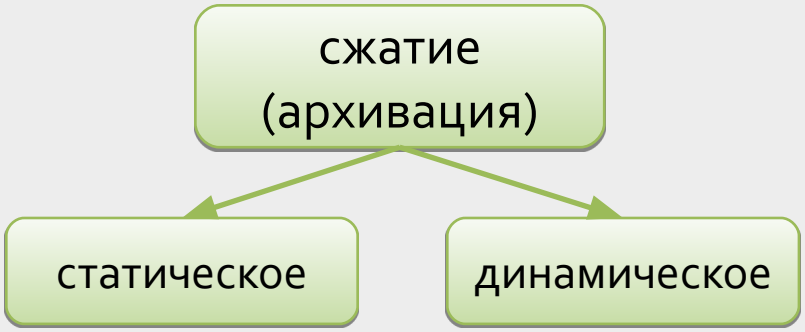


Криптографические методы



- моноалфавитная
- полиалфавитная
- гомофоническая
- полиграммная





Популярные антивирусные программы

KASPERSKY ANTI-VIRUS

avast!

Dr.WEB

Norton AntiVirus™