Информационные и компьютерные угрозы разнообразны и постоянно эволюционируют вместе с технологиями. Они могут привести к нарушению конфиденциальности, доступности и целостности данных, вызвать материальный ущерб и даже стать причиной серьёзных последствий для организаций и частных лиц. Вот основные виды угроз:

1. Вредоносное программное обеспечение (malware):

* **Компьютерные вирусы**: Заражение компьютеров, ведущих к повреждению данных или передаче информации злоумышленнику.
* **Шпионское ПО (spyware)**: Незаметное отслеживание действий пользователя и передача данных третьим лицам.
* **Руткиты (rootkits)**: Скрывающиеся глубоко в системе программы, позволяющие злоумышленникам удалённо управлять заражённым устройством.
* **Вымогательское ПО (ransomware)**: Блокировка доступа к файлам и требование выкупа за восстановление доступа.
* **Рекламное ПО (adware)**: Ненужные рекламные окна, снижающие удобство использования устройства.

2. Фишинг и социальная инженерия:

* **Фишинг**: Массовая рассылка писем или сообщений, маскирующихся под уведомления банков, служб доставки или знакомых, с целью похищения паролей, реквизитов карт и других чувствительных данных.
* **Спуфинг (spoofing)**: Подмена адресов отправителей электронных писем, номеров телефонов или IP-адресов, чтобы ввести жертву в заблуждение относительно подлинности ресурса.
* **Атаки методом подбора пароля (brute force attacks)**: Автоматизированные попытки входа путём перебора возможных комбинаций паролей.

3. Боты и ботнеты:

* **Ботнеты**: Сети заражённых компьютеров («ботов»), управляемых одним центром, используемых для массовой рассылки спама, проведения DDoS-атак или майнинга криптовалют.
* **DOS/DDoS-атаки**: Перегрузка серверов потоком ложных запросов, ведущая к невозможности легитимных пользователей пользоваться сервисом.

4. SQL-инъекции и XSS-уязвимости:

* **SQL-инъекция**: Внедрение произвольных команд в базу данных через некорректно обработанные запросы, позволяющее похитить или изменить информацию.
* **XSS (Cross-Site Scripting)**: Запуск вредоносного JavaScript-кода на сайте жертвы, позволяющий перехватывать сессии авторизации или вводить другие команды.

5. Несанкционированный доступ и инсайдерские угрозы:

* **Взлом учётных записей**: Получение несанкционированного доступа к личным аккаунтам или внутренним ресурсам организаций.
* **Инсайдеры**: Сотрудники или партнёры, намеренно или случайно допускающие утечку конфиденциальной информации.

6. Недостаточная защищённость IoT-устройств:

* Многие устройства интернета вещей (умные телевизоры, камеры видеонаблюдения, бытовые приборы) обладают слабыми средствами защиты, что создаёт дополнительные точки проникновения для злоумышленников.

7. Кража идентификационной информации (identity theft):

* Похищение паспортных данных, банковских счетов, медицинской информации с последующим использованием их в корыстных целях.

8. Недобросовестные сотрудники (insiders):

* Нарушение политики безопасности сотрудниками, приведшее к потере или компрометации важной информации.

9. Потеря физического контроля над оборудованием:

* Кража ноутбуков, смартфонов или USB-накопителей с хранящимися там ценными данными.

10. Отсутствие резервного копирования и катастрофоустойчивых мер:

* Невозможность восстановления утраченных данных после сбоя оборудования или инцидента безопасности.

Каждая из перечисленных угроз потенциально может иметь серьезные последствия, включая потерю репутации, финансовых потерь, нарушения законодательства и нарушение бизнес-процессов. Чтобы минимизировать риск воздействия таких угроз, важно применять современные защитные меры, регулярно обновлять антивирусные программы, своевременно устранять уязвимости и повышать общий уровень компьютерной грамотности.