# Объекты уязвимости. Дестабилизирующие факторы и угрозы надежности

Самыми частыми и опасными являются непреднамеренные ошибки пользователей, операторов и системных администраторов, обслуживающих КИС.

Такие ошибки приводят к прямому ущербу, а иногда создают слабые места, которыми могут воспользоваться злоумышленники.

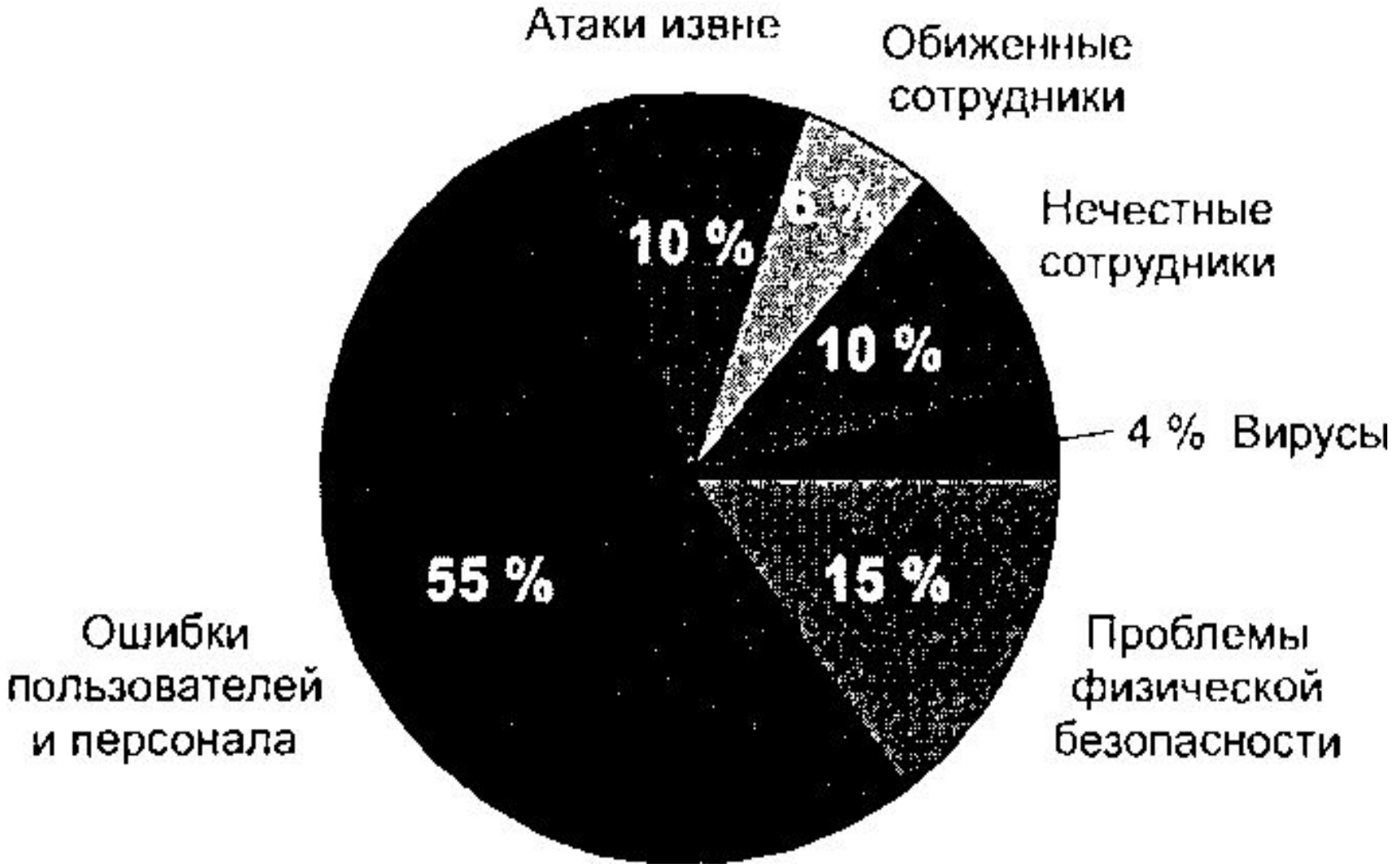



**Рис. 1. Источники нарушений безопасности**

**Угроза** - *это потенциально возможное событие, явление или процесс, которое посредством воздействия на компоненты информационной системы может привести к нанесению ущерба*

**Уязвимость** - *это любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.*

**Атака -** *это любое действие нарушителя, которое приводит к реализации угрозы путём использования уязвимостей информационной системы.*

# Источники возникновения уязвимостей

- Уязвимости закладываются на этапе проектирования
- Уязвимости возникают на этапе реализации (программирования).
- Уязвимости являются следствием ошибок, допущенных в процессе эксплуатации информационной системы.

# Группы участников процесса управления уязвимостями

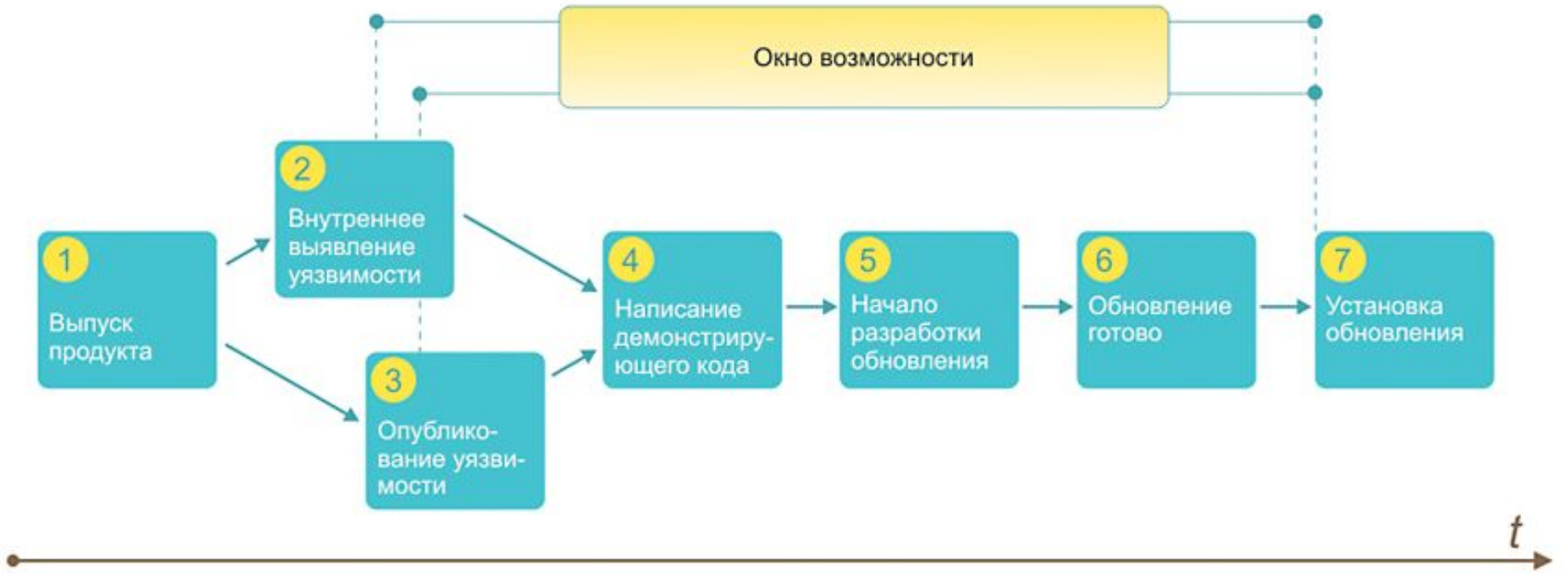
**Исследователи** которые, обнаруживают дыры в системах и продуктах, подразделяются на 2 основных категории – «white hat» и «black hat». Первые сообщают разработчику об уязвимости, не публикуя при этом где-либо информацию о ней. Вторые – предоставляет информацию авторам вредоносного ПО.

**Производители** (vendors) – создатели ИС и программных продуктов.

**Пользователи**, которые не только вынуждены использовать уязвимые системы в своей работе, но и сами зачастую обнаруживают дыры в используемом программном обеспечении.

**Координаторы** (специальные группы или организации, координирующие весь процесс (например, CERT/CC, Cisco PSIRT, FIRST и т.д.)).

# Этапы жизненного цикла уязвимостей



# Классификация уязвимостей информационных систем по этапам жизненного цикла

| Категории уязвимостей по этапам жизненного цикла АС | Сложность обнаружения | Сложность устранения |
|---|---|---|
| уязвимости проектирования | трудоемкий и длительный процесс | трудоемкий и длительный процесс, иногда устранение невозможно |
| уязвимости реализации | относительно трудно и долго | несложно, но относительно долго |
| уязвимости конфигурации | легко и быстро | легко и быстро |

# Классификация угроз по аспекту информационной безопасности

1. Угрозы нарушения конфиденциальности;
2. Угроза нарушения целостности;
3. Угроза доступности.

# Классификация угроз по непосредственному источнику угроз

1. **Угрозы непосредственным источником которых является природная среда** (объективные физические процессы или стихийные природные явления, независящие от человека: стихийные бедствия, магнитные бури, радиоактивное излучение).

2. **Угрозы непосредственным источником которых является человек** (персонал АС, нарушители).

# Классификация угроз по степени преднамеренности проявления

1. **Угрозы случайного действия** и/или угрозы, вызванные ошибками или халатностью персонала:
- проявление ошибок программно-аппаратных средств АС;
- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
- неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов или программ);
- неправомерное включение оборудования или изменение режимов работы устройств и программ;
- неумышленная порча носителей информации;
- пересылка данных по ошибочному адресу абонента (устройства);
- ввод ошибочных данных;
- неумышленное повреждение каналов связи.

2. **Угрозы преднамеренного действия** (например, угрозы действий нарушителя для хищения информации).

# Классификация угроз по положению источника угроз

1. **Угрозы источник которых расположен вне контролируемой зоны территории** (помещения), на которой находится АС:
- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания и отопления);
- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
- дистанционная фото и видеосъемка.

# Классификация угроз по положению источника угроз

2. **Угрозы источник которых расположен в пределах контролируемой зоны территории** (помещения), на которой находится АС:

- хищение производственных отходов (распечаток, записей, списанных носителей информации);
- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи);
- применение подслушивающих устройств.

3. **Угрозы источник которых имеет доступ к периферийным устройствам АС**.

# Классификация угроз по степени зависимости от активности АС

1. **Угрозы которые могут проявляться независимо от активности АС**:
- вскрытие шифров криптозащиты информации;
- хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и компьютерных систем).
2. **Угрозы которые могут проявляться только в процессе автоматизированной обработки данных** (например, угрозы выполнения и распространения программных вирусов).

# Классификация угроз по степени воздействия на АС

1. **Пассивные угрозы**, которые при реализации ничего не меняют в структуре и содержании АС (например, угроза копирования секретных данных);
2. **Активные угрозы**, которые при воздействии вносят изменения в структуру и содержание АС:
- внедрение аппаратных спецвложений, программных "закладок" и "вирусов", т.е. таких участков программ, которые не нужны для выполнения заявленных функций, но позволяют преодолеть систему защиты, скрытно и незаконно осуществить доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;
- действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы);
- угроза умышленной модификации информации.

# Модель нарушителя информационной безопасности

**Модель нарушителя** — абстрактное описание нарушителя информационной безопасности.

**Модель нарушителя определяет**:

- категории (типы) нарушителей, которые могут воздействовать на объект;
- цели, которые могут преследовать нарушители каждой категории;
- возможный количественный состав;
- используемые инструменты, принадлежности, оснащение;
- типовые сценарии возможных действий, описывающие последовательность (алгоритм) действий групп и отдельных нарушителей, способы их действий на каждом этапе и т.д.

# Классификация атак

Производя атаку, злоумышленник преследует определённые цели:

- нарушение нормального функционирования объекта атаки (отказ в обслуживании)
- получение контроля над объектом атаки
- получение конфиденциальной и критичной информации
- модификация и фальсификация данных

# Классификация атак по мотивации действий

- Случайность
- Безответственность
- Самоутверждение
- Идейные соображения
- Вандализм
- Принуждение
- Месть
- Корыстный интерес

# Механизмы реализации атак

- пассивное прослушивание

  *Пример: перехват трафика сетевого сегмента*

- подозрительная активность

  *Пример: сканирование портов (служб) объекта атаки, попытки подбора пароля*

- бесполезное расходование вычислительного ресурса

  *Пример: исчерпание ресурсов атакуемого узла или группы узлов, приводящее к снижению производительности (переполнение очереди запросов на соединение и т.п.)*

- нарушение навигации (создание ложных объектов и маршрутов)

  *Пример: Изменение маршрута сетевых пакетов, таким образом, чтобы они проходили через хосты и маршрутизаторы нарушителя, изменение таблиц соответствия условных Internet - имен и IP -адресов (атаки на DNS ) и т.п.*

• Выведение из строя

*Пример: посыпка пакетов определённого типа на атакуемый узел, приводящая к отказу узла или работающей на нём службы.*

• Запуск приложений на объекте атаки

*Пример: выполнение враждебной программы в оперативной памяти объекта атаки (троянские кони, передача управления враждебной программе путём переполнения буфера, исполнение вредоносного мобильного кода на Java или ActiveX и др.)*

Для защиты от атак необходимо использовать комплекс средств безопасности, реализующий основные защитные механизмы и состоящий из следующих компонентов:

- Межсетевые экраны, являющиеся первой линией обороны и реализующие комплекс защитных механизмов, называемый защитой периметра.
- Средства анализа защищённости, позволяющие оценить эффективность работы средств защиты и обнаружить уязвимости узлов, протоколов, служб.
- Средства обнаружения атак, осуществляющие мониторинг в реальном режиме времени.