

The background features several large, stylized, overlapping swirls in light green, light blue, and light purple. Interspersed among these swirls are numerous small, yellow, starburst-like shapes, some of which are larger and more prominent than others. The overall aesthetic is clean and modern.

Виды угроз ИС



Угрозы безопасности информации

- Под угрозой (вообще) обычно понимают потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.



Угрозы ИС

Технологические

– Физические

- Человек
- Форс-мажоры
- Отказ оборудования

– Логические

- Локальный нарушитель
- Удаленный нарушитель

• Организационные

– Воздействие на персонал

- Физическое воздействие
- Психологическое воздействие

– Действия персонала

- Умышленные
- Неумышленные



Классификация угроз безопасности

Угрозы безопасности

```
graph TD; A[Угрозы безопасности] --> B[Естественные]; A --> C[Искусственные]; C --> D[Преднамеренные]; C --> E[Непреднамеренные];
```

Естественные

Искусственные

Преднамеренные

Непреднамеренные

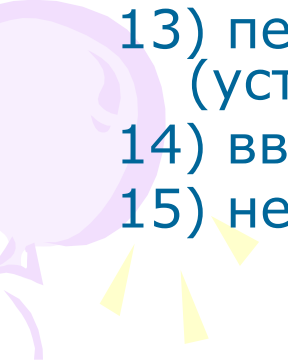


Непреднамеренные искусственные угрозы

- 1) действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы;
- 2) отключение оборудования или изменение режимов работы устройств и программ;
- 3) неумышленная порча носителей информации;
- 4) запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы;
- 5) нелегальное внедрение и использование неучтенных программ;
- 6) заражение компьютера вирусами;



Непреднамеренные искусственные угрозы

- 7) действия, приводящие к разглашению конфиденциальной информации;
 - 8) разглашение, передача или утрата атрибутов разграничения доступа;
 - 9) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
 - 10) игнорирование ограничений при работе в системе;
 - 11) вход в систему в обход средств защиты;
 - 12) некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
 - 13) пересылка данных по ошибочному адресу абонента (устройства);
 - 14) ввод ошибочных данных;
 - 15) неумышленное повреждение каналов связи.
- 

Основные преднамеренные искусственные угрозы

- 1) физическое разрушение системы или вывод из строя компонентов компьютерной системы
- 2) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем;
- 3) действия по дезорганизации функционирования системы
- 4) внедрение агентов в число персонала системы
- 5) вербовка персонала или отдельных пользователей, имеющих определенные полномочия;
- 6) применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;
- 7) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
- 8) перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена;
- 9) хищение носителей информации;
- 10) несанкционированное копирование носителей информации;

Основные преднамеренные искусственные угрозы

- 11) хищение производственных отходов;
- 12) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- 13) чтение информации из областей оперативной памяти;
- 14) незаконное получение паролей и других реквизитов разграничения доступа;
- 15) несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;
- 16) вскрытие шифров криптозащиты информации;
- 17) внедрение аппаратных спецвложений, программных "закладок" и "вирусов";
- 18) незаконное подключение к линиям связи



Модель нарушителя в АС

При разработке модели нарушителя определяются

- · предположения о категориях лиц, к которым может принадлежать нарушитель;
- · предположения о мотивах действий нарушителя (преследуемых нарушителем целях);
- · предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);
- · ограничения и предположения о характере возможных действий нарушителей.



Нарушитель

- Внешний

- клиенты (представители организаций, граждане);
- посетители (приглашенные по какому-либо поводу);
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.);
- представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;
- лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность АС);
- любые лица за пределами контролируемой территории.

- Внутренний

- пользователи (операторы) системы;
- персонал, обслуживающий технические средства (инженеры, техники);
- сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты);
- технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты АС);
- сотрудники службы безопасности АС;
- руководители различных уровней должностной иерархии.



Локальный и удаленный нарушитель

- Использует вредоносные программы:
 - Логические бомбы
 - Троянский конь
 - Вирус
 - Червь
 - Захватчик паролей
 - и т.д.