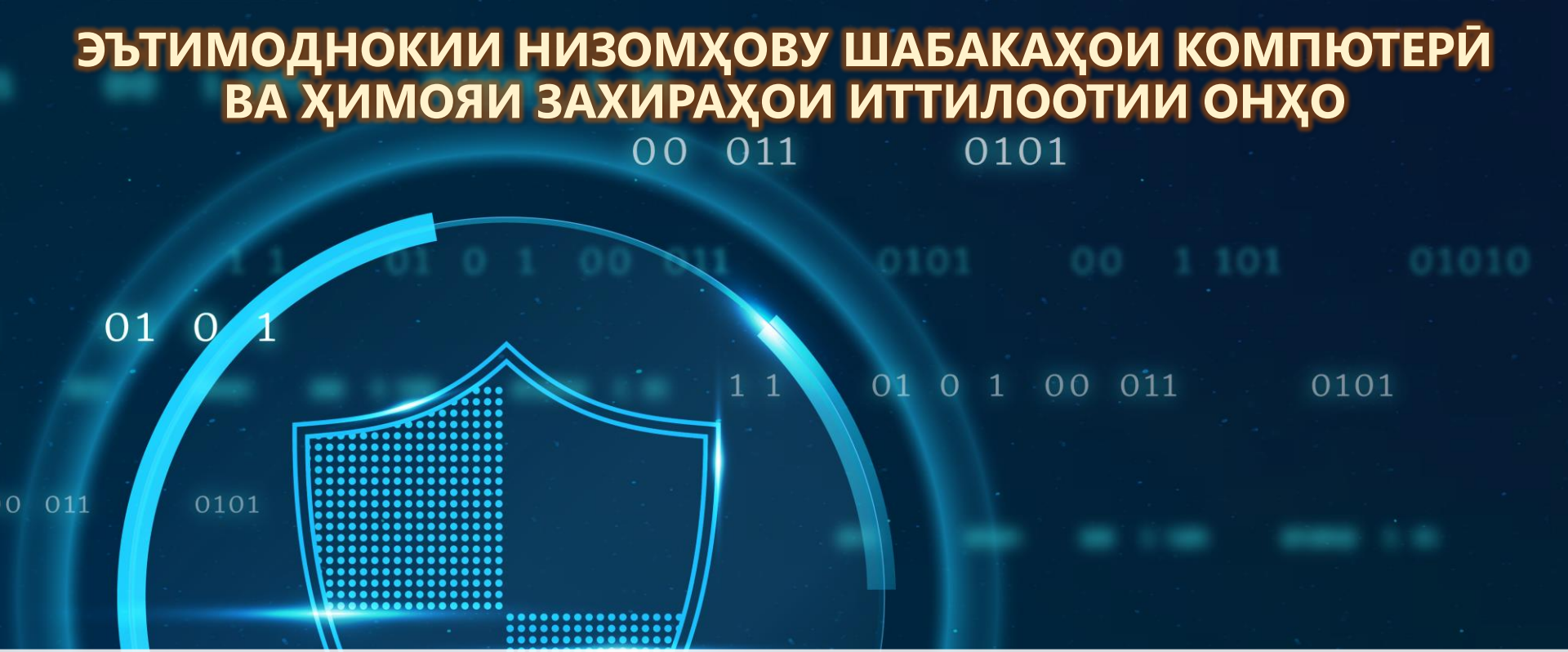
ЭЪТИМОДНОКИИ НИЗОМҲОВУ ШАБАКАҲОИ КОМПЮТЕРӢ ВА ҲИМОЯИ ЗАХИРАҲОИ ИТТИЛООТИИ ОНҲО



Тема 2: Угрозы безопасности в компьютерных системах

Составитель: Назаров А.А.

Содержание

- Понятие и классификация угроз
- Модель угроз, модель нарушителя
- Человеческий фактор в угрозах безопасности

Понятие и классификация угроз

Одним из важнейших аспектов проблемы обеспечения безопасности компьютерных систем является определение, анализ и классификация возможных угроз безопасности АС. Перечень значимых угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для проведения анализа рисков и формулирования требований к системе защиты АС.

Угроза информационной безопасности совокупность условий и факторов, создающих опасность нарушения информационной безопасности.

Угрозы безопасности информации — это некая совокупность факторов и условий, которые создают опасность в отношении защищаемой информации.

Для того чтобы определить угрозы, от которых необходимо обезопасить информацию, нужно определить объекты защиты.

Понятие и классификация угроз

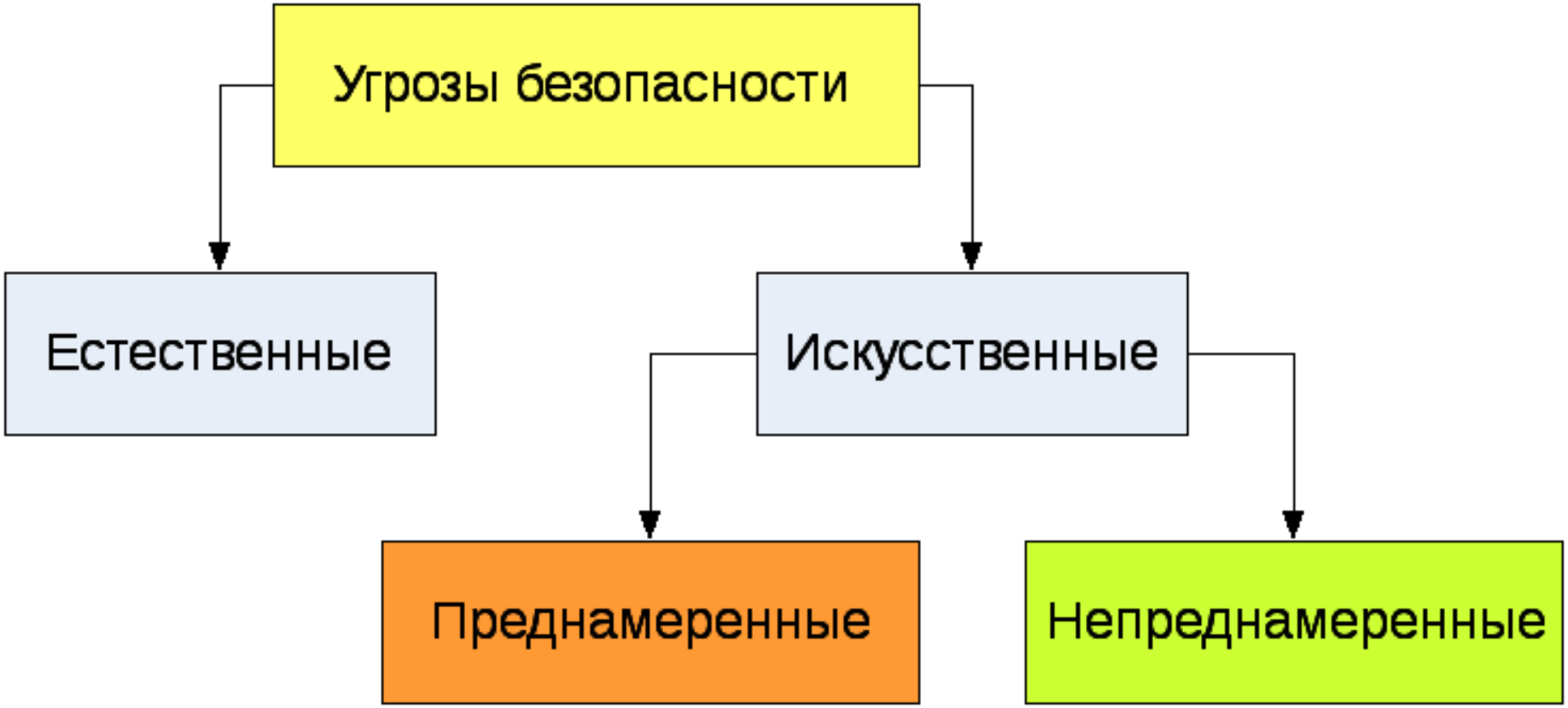
Угроза безопасности КС – совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности, [правомерной] доступности КИ и/или снижения надежности [безотказности и аутентичности] реализации функций КС

Понятие и классификация угроз

Угроза информационной безопасности (ИБ) – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам. Согласно статистике применительно к этим угрозам, можно привести следующие данные (по результатам исследований, проведённых в России компанией InfoWath):

- ❖ Кража информации – 64%
- ❖ Вредоносное ПО – 60%
- ❖ Хакерские атаки – 48%
- ❖ Спам – 45%
- ❖ Халатность сотрудников – 43%
- ❖ Аппаратные и программные сбои – 21%
- ❖ Кража оборудования – 6%
- ❖ Финансовое мошенничество – 5%

Понятие и классификация угроз



Понятие и классификация угроз

Естественные угрозы – это угрозы, вызванные воздействиями на автоматизированную систему и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека

Искусственные угрозы – это угрозы информационной безопасности, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

1. **Непреднамеренные** (неумышленные, случайные) угрозы, вызванные ошибками в проектировании автоматизированной системы и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п..

2. **Преднамеренные** (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников).

Понятие и классификация угроз

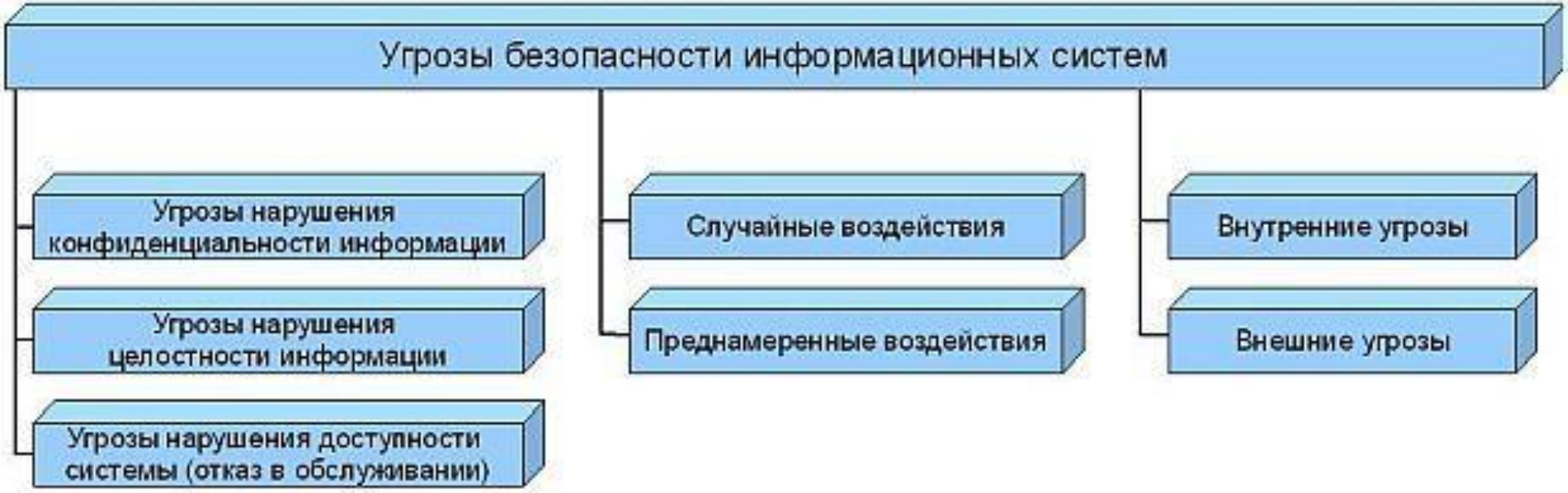
Попытка реализации угрозы называется атакой.

Классификация угроз ИБ можно выполнить по нескольким критериям:

- **по аспекту ИБ** (доступность, целостность, конфиденциальность);
- **по компонентам ИС**, на которые угрозы нацелены (данные, программа, аппаратура, поддерживающая инфраструктура);
- **по способу осуществления** (случайные или преднамеренные действия природного или техногенного характера);
- **по расположению источника** угроз (внутри или вне рассматриваемой ИС).

Типы информационных угроз

Понятие и классификация угроз



Типы информационных угроз

Понятие и классификация угроз

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались. **Типы и субъекты угроз**

№	Тип угроз	Оператор	Руководитель	Программист	Инженер (техник)	Пользователь	Конкурент
1.	Изменение кодов	+		+			
2.	Копирование файлов	+		+			
3.	Уничтожение файлов	+	+	+		+	+
4.	Присвоение программ			+	+		+
5.	Шпионаж	+	+	+			+
6.	Установка подслушивания			+	+		+
7.	Саботаж	+		+	+		+
8.	Продажа данных	+	+	+		+	
9.	Воровство		+	+		+	+

Понятие и классификация угроз

Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место, когда получен доступ к некоторой информации ограниченного доступа, хранящейся в вычислительной системе или передаваемой от одной системы к другой. В связи с угрозой нарушения конфиденциальности, используется термин «утечка». Подобные угрозы могут возникать вследствие «человеческого фактора» (например, случайное делегировании тому или иному пользователю привилегий другого пользователя), сбоев работе программных и аппаратных средств.

Понятие и классификация угроз

Угрозы нарушения целостности – это угрозы, связанные с вероятностью модификации той или иной информации, хранящейся в информационной системе. Нарушение целостности может быть вызвано различными факторами – от умышленных действий персонала до выхода из строя оборудования.

Угрозы доступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы).

Нарушение доступности представляет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес-целей.

Понятие и классификация угроз

Угрозы нарушения доступности системы (отказ в обслуживании) направлены на создание таких ситуаций, когда определённые действия либо снижают работоспособность информационной системы, либо блокируют доступ к некоторым её ресурсам. **Причины случайных воздействий:**

- **аварийные ситуации** из-за стихийных бедствий и отключения электроэнергии;
- **ошибки в программном обеспечении;**
- ошибки в работе обслуживающего персонала и пользователей;
- помехи в линии связи из-за воздействия внешней среды, а также вследствие плотного трафика в системе (характерно для беспроводных решений).

Понятие и классификация угроз

Преднамеренные воздействия связаны с целенаправленными действиями злоумышленника, в качестве которого может выступить любое заинтересованное лицо (конкурент, посетитель, персонал и т.д.). Действия злоумышленника могут быть обусловлены разными мотивами: недовольством сотрудника своей карьерой, материальным интересом, любопытством, конкуренцией, стремлением самоутвердиться любой ценой и т.п.

Понятие и классификация угроз

Внутренние угрозы инициируются персоналом объекта, на котором установлена система, содержащая конфиденциальную информацию. Причинами возникновения таких угроз может послужить нездоровый климат в коллективе или неудовлетворенность от выполняемой работы некоторых сотрудников, которые могут предпринять действия по выдаче информации лицам, заинтересованным в её получении.

Понятие и классификация угроз

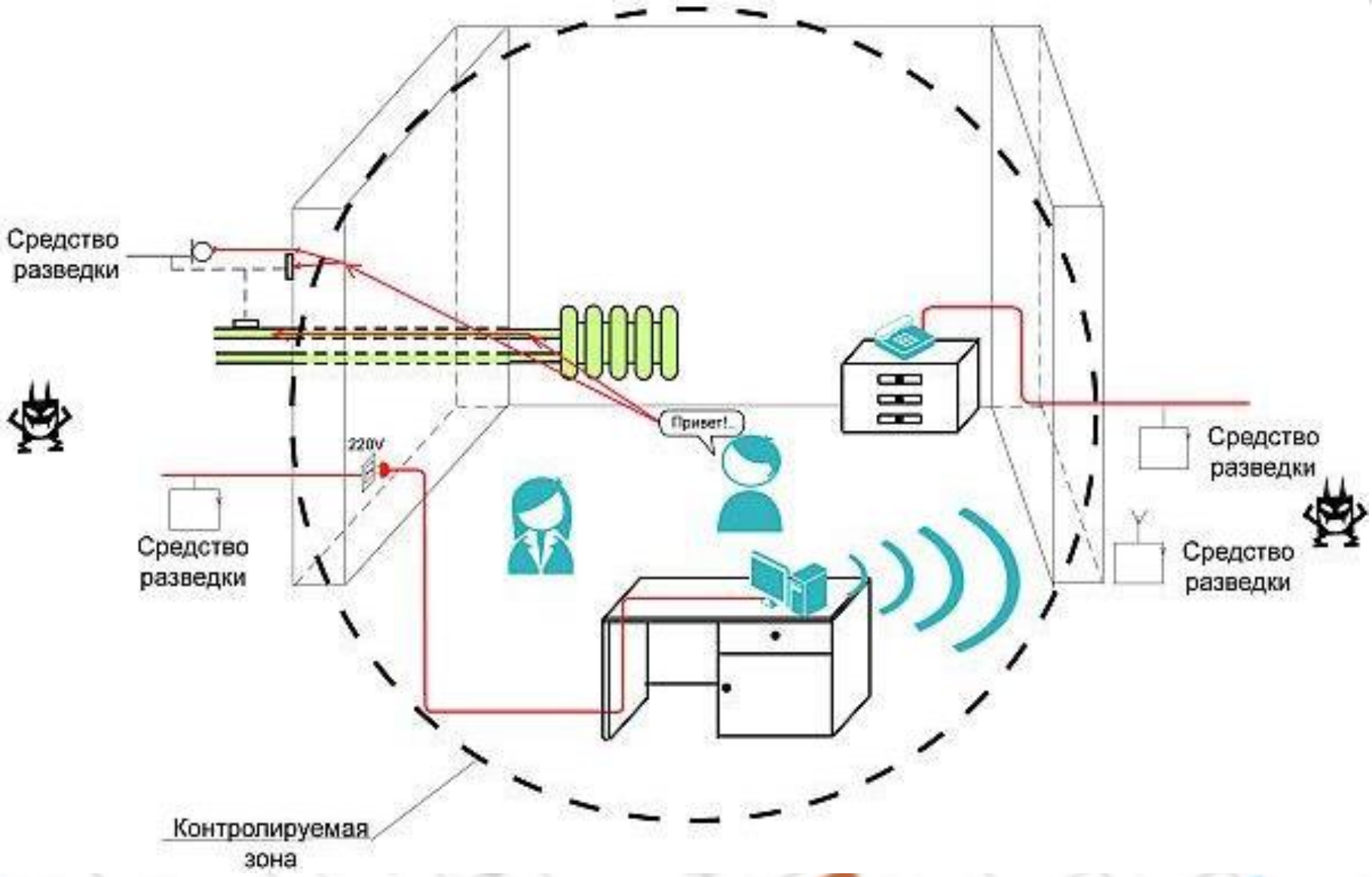
Под **внешними угрозами безопасности** понимаются угрозы, созданные сторонними лицами и исходящие из внешней среды, такие как:

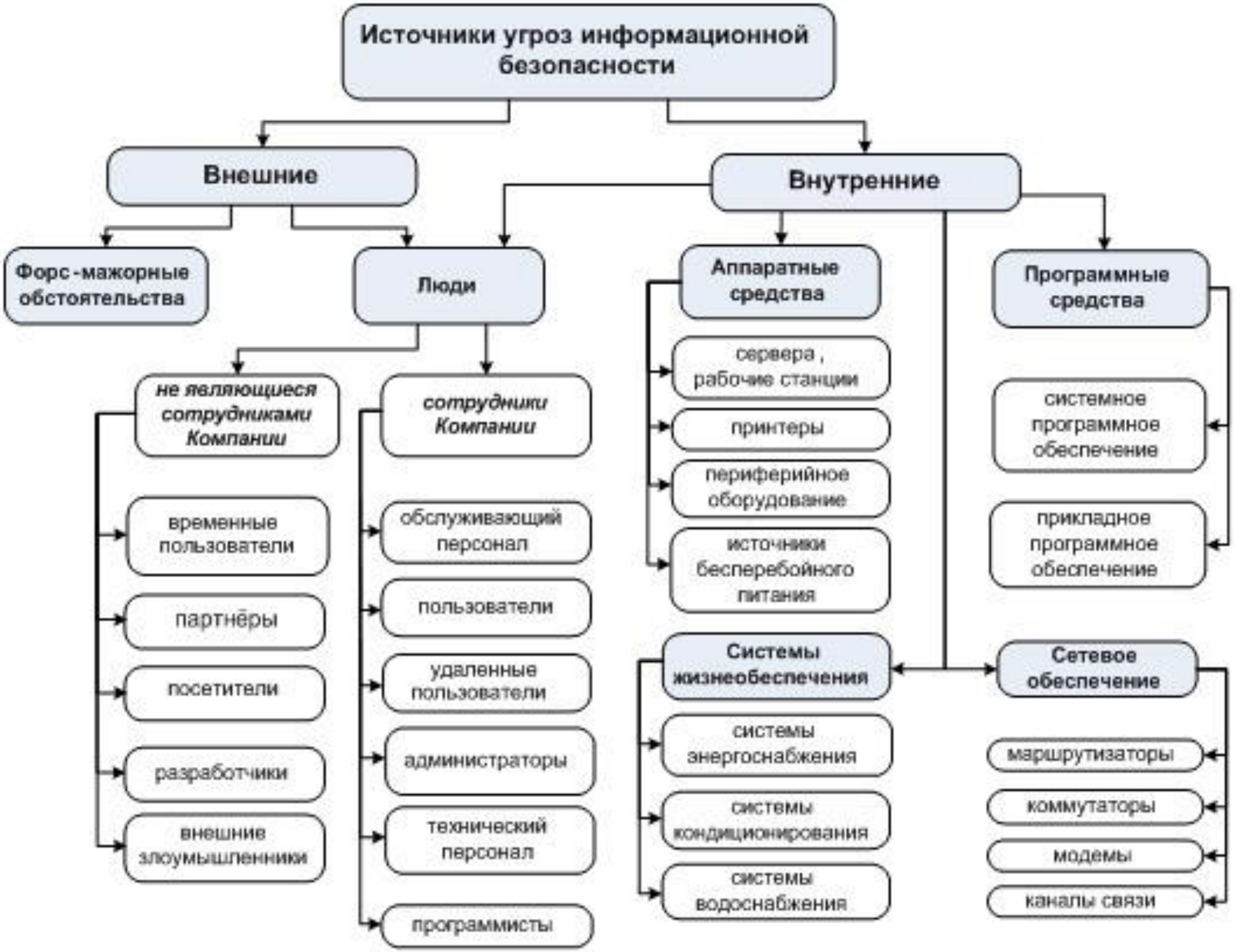
- ❖атаки из внешней сети (например, Интернет);
- ❖распространение вредоносного программного обеспечения;
- ❖нежелательные рассылки (спам);
- ❖воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения в информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем;

Понятие и классификация угроз

- перехват информации с использованием радиоприемных устройств;
- воздействие на информацию, осуществляемое путем несанкционированного использования сетей инженерных коммуникаций;
- воздействие на персонал предприятия с целью получения конфиденциальной информации.

Классификация угроз




Источники угроз информационной безопасности
Внешние
Внутренние
Форс-мажорные обстоятельства
Люди
Аппаратные средства
Программные средства
не являющиеся сотрудниками Компании
сотрудники Компании
сервера, рабочие станции
принтеры
периферийное оборудование
источники бесперебойного питания
системное программное обеспечение
прикладное программное обеспечение
временные пользователи
партнёры
посетители
разработчики
внешние злоумышленники
обслуживающий персонал
пользователи
удаленные пользователи
администраторы
технический персонал
программисты
Системы жизнеобеспечения
Сетевое обеспечение
системы энергоснабжения
системы кондиционирования
системы водоснабжения
маршрутизаторы
коммутаторы
модемы
каналы связи

Модель угроз, модель нарушителя

Модель угроз – это перечень возможных угроз.

Модель угроз (безопасности информации) – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Итак, **модель угроз** – это документ, тем или иным способом описывающий возможные угрозы безопасности персональных данных.

Модель угроз безопасности персональных данных необходима для определения требований к системе защиты. Без модели угроз невозможно построить адекватную (с точки зрения денежных затрат) систему защиты информации, обеспечивающую безопасность персональных данных.

Модель угроз, модель нарушителя

Зачем нужна модель угроз

Модель угроз безопасности персональных данных необходима для определения требований к системе защиты. Без модели угроз невозможно построить адекватную (с точки зрения денежных затрат) систему защиты информации, обеспечивающую безопасность персональных данных.

В систему защиты включаются только те средства защиты информации, которые нейтрализуют актуальные угрозы.

Модель угроз, модель нарушителя

Модель угроз (или как ее еще называют "Частная модель угроз") может разрабатываться ответственными за защиту персональных данных в организации. Также могут привлекаться сторонние эксперты. Разработчики модели угроз должны владеть полной информацией об информационной системе персональных данных, знать нормативную базу по защите информации.

При отсутствии экспертов разработку модели угроз лучше доверить сторонней организации.