

Угрозы безопасности
компьютерных систем и
информационно-коммуникационных
технологий

Угрозы безопасности в компьютерных системах

1. Понятие угроз безопасности, их классификация и идентификация
 1. Методы оценивания угроз
-

Угрозы безопасности КС

- Угроза – потенциальная возможность нарушить ИБ.
 - Атака – попытка реализации угрозы
 - *Угроза* - следствие наличия *уязвимостей* в защите ИС
 - **Окно опасности** - промежуток времени от момента, когда появляется возможность использовать уязвимость, до момента, когда она ликвидируется

 - Угрозы безопасности – исходный фактор для выбора защитных механизмов при создании защищенных КС.
 - **Угроза безопасности КС** –
 - *совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения*
 - *конфиденциальности,*
 - *целостности,*
 - *[правомерной] доступности информации и/или снижения надежности [безотказности и аутентичности] реализации функций КС*
-

Систематизация и классификация угроз

систематизация

- *приведение в систему, т.е. в нечто целое, представляющее собой единство закономерно расположенных и находящихся во взаимной связи частей; выстраивание в определенный порядок*

классификация

- *последовательное деление понятий (предметов исследования), проводимое по характеристикам и параметрам, существенным с точки зрения исследовательской задачи*
 - *Частный случай систематизации*
-

Методы и цели классификации

- Таксономическая (родовая, дерево)
 - $O = O1 \cup O2, O1 \cap O2 = \emptyset$
 - Мереологическая ("часть-целое")
 - Цели классификации
 - теоретико-познавательные функции
 - прикладные функции
 - обеспечивают полноту анализа при идентификации угроз для конкретной КС
 - позволяют систематизировать выбор защитных мер, которые могут устранять сразу целый класс (с соответствующими подклассами) угроз
-

Угрозы

A

по природе происхождения

Случайные
(объективные)

Преднамеренные
(субъективные)

B

по направлению осуществления

Внешние

Внутренние

C

по объекту воздействия

АРМ
польз-лей

АРМ
адм-в

Средства
отображ.

Средства
документ.

Средства
загр. ПО

Каналы
связи

D

по способу осуществления

Информационные

Программно-аппаратные

Физические

Радиоэлектронные

Организационно-правовые

E

по жизн. циклу ИС

Разр. и произв.
апп. прог. ср.

Проект. и ввод
КС в экспл.

Эксплуатация
КС

Вывод из
экспл. КС

Каталогизация угроз

- Составление и закрепление в стандартах таксономически-классификационных схем угроз. Например, ГОСТ **51275-99** «Защита информации. Объект информатизации. Факторы, воздействующие на информацию»
 - Используется для идентификации угроз
 - Идентификация включает
 - выделение угроз, характерных для конкретной КС
 - Их идентификацию (присвоения кодов)
 - **спецификацию** (описание) угроз по некоторым параметрам:
 - источник (природу происхождения) угрозы, активы (объекты КС), на которые направлена угроза), способы осуществления угрозы, возможные уязвимости, которые м.б. использованы для реализации угрозы.
 - В дальнейшем – для выбора защитных мер, методов и механизмов обеспечения безопасности при создании и эксплуатации конкретных защищенных КС
-

Классы, подклассы и группы факторов (ГОСТ Р 51275-99)

Объективные

Внутренние

Передача сигналов по проводным линиям связи

Передача сигналов по оптико-волоконным линиям связи

Излучение сигналов, функционально-присущих ОИ

ПЭМИ

Паразитные электромагнитные излучения

Наводки

Акустоэлектрические преобразования в элементах ТС ОИ

Дефекты, сбои, аварии ТС и систем ОИ

Дефекты, сбои и отказы программного обеспечения ОИ

Явления техногенного характера

Природные явления, стихийные бедствия

Внешние

Субъективные

Внутренние

Разглашение ЗИ лицами, имеющими к ней право доступа

Неправомерные действия со стороны лиц, имеющих право доступа к ЗИ

НСД к ЗИ (внутренний)

Неправильное организационное обеспечение ЗИ

Неправильное организационное обеспечение ЗИ

Ошибки обслуживающего персонала ОИ

Доступ к ЗИ с применением технических средств

НСД к ЗИ (внешний)

Блокирование доступа к ЗИ путем перегрузки технических средств обработки информации ложными заявками на ее обработку

Действия криминальных групп и отдельных преступных элементов

Пример. Угрозы по природе происхождения. Случайные

- Отказы и сбои аппаратуры
 - *определяются качеством и надежностью аппаратуры*
 - *техническими решениями и др. факторами*
- Помехи на линиях связи от внешних воздействий
 - *правильность выбора места (маршрута) прокладки*
 - *технических решений по помехозащищенности*
 - *э/м обстановки*
- Ошибки человека как звена информационной системы

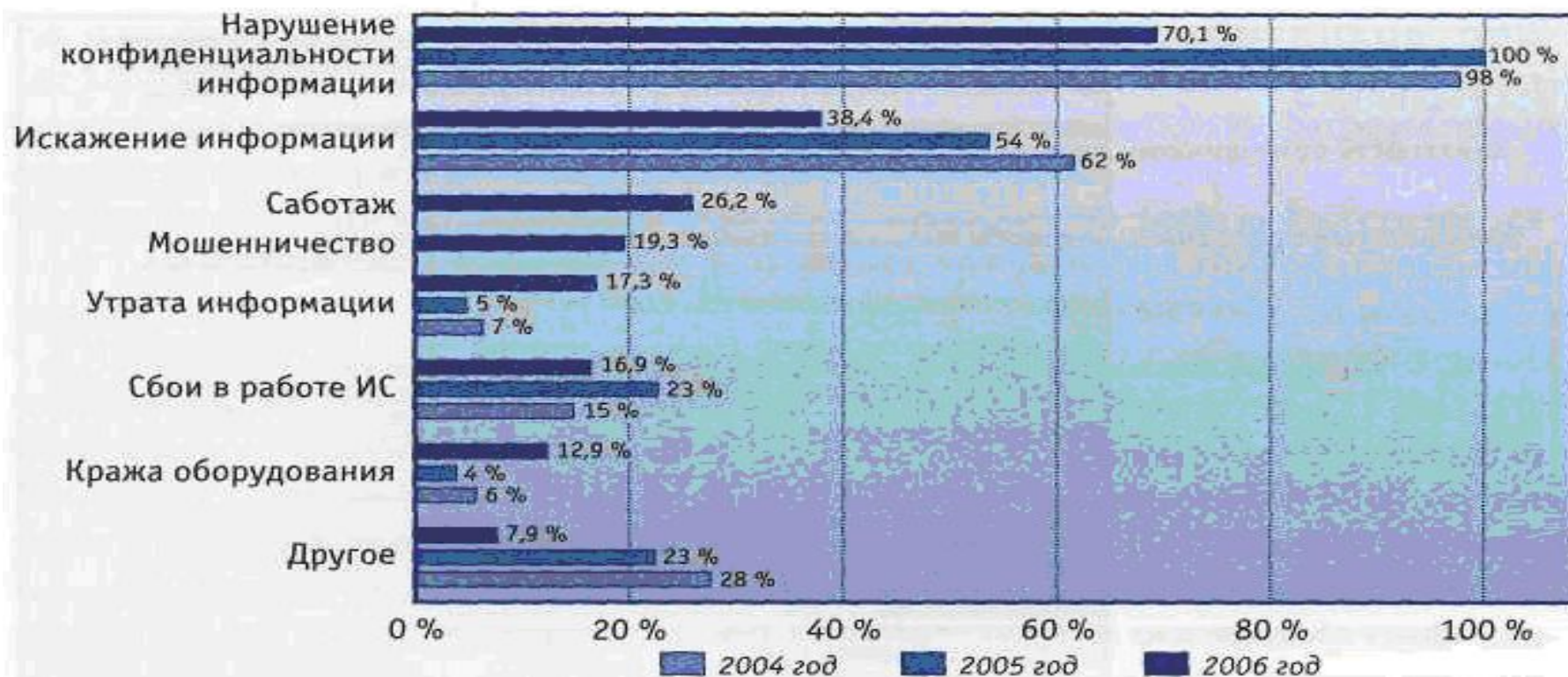
По месту в системе	По типу
<ul style="list-style-type: none">- <i>как источника информации</i>- <i>как оператора (ввод-вывод данных)</i>- <i>как обслуживающего персонала</i>- <i>как звена принятия решений</i> <p>Интенсивность - $2 \cdot 10^{-2} \dots 4 \cdot 10^{-3}$</p>	<ul style="list-style-type: none">- <i>логические (неправильные решения)</i>- <i>сенсорные (неправильное восприятие)</i>- <i>оперативные и моторные (неправильная реализация или реакция)</i>

Пример. Угрозы по природе происхождения. Случайные

- Схемные и системотехнические ошибки разработчиков
- Структурные, алгоритмические и программные ошибки
 - *специальные методы проектирования и разработки*
 - *специальные процедуры тестирования и отладки*
- Аварийные ситуации
 - *- по выходу из строя электропитания*
 - *- по стихийным бедствиям*
 - *- по выходу из строя систем жизнеобеспечения*

Пример. Преднамеренные угрозы. Инциденты в ИТ-сфере РФ

- вызванные человеком или связанные с действиями человека, определяются т.н. человеческим фактором (мотивы, категории, возможности)



Угрозы по направлению осуществления

- **Внешние**
 - *исходящие извне по отношению к персоналу, к организации (предприятию), к государству, к территории (зданиям, помещениям) КС*
- **Внутренние**
 - *происходящие внутри КС, среди персонала, в зоне расположения объектов КС*

**Внешняя
(неконтролируемая)
зона**

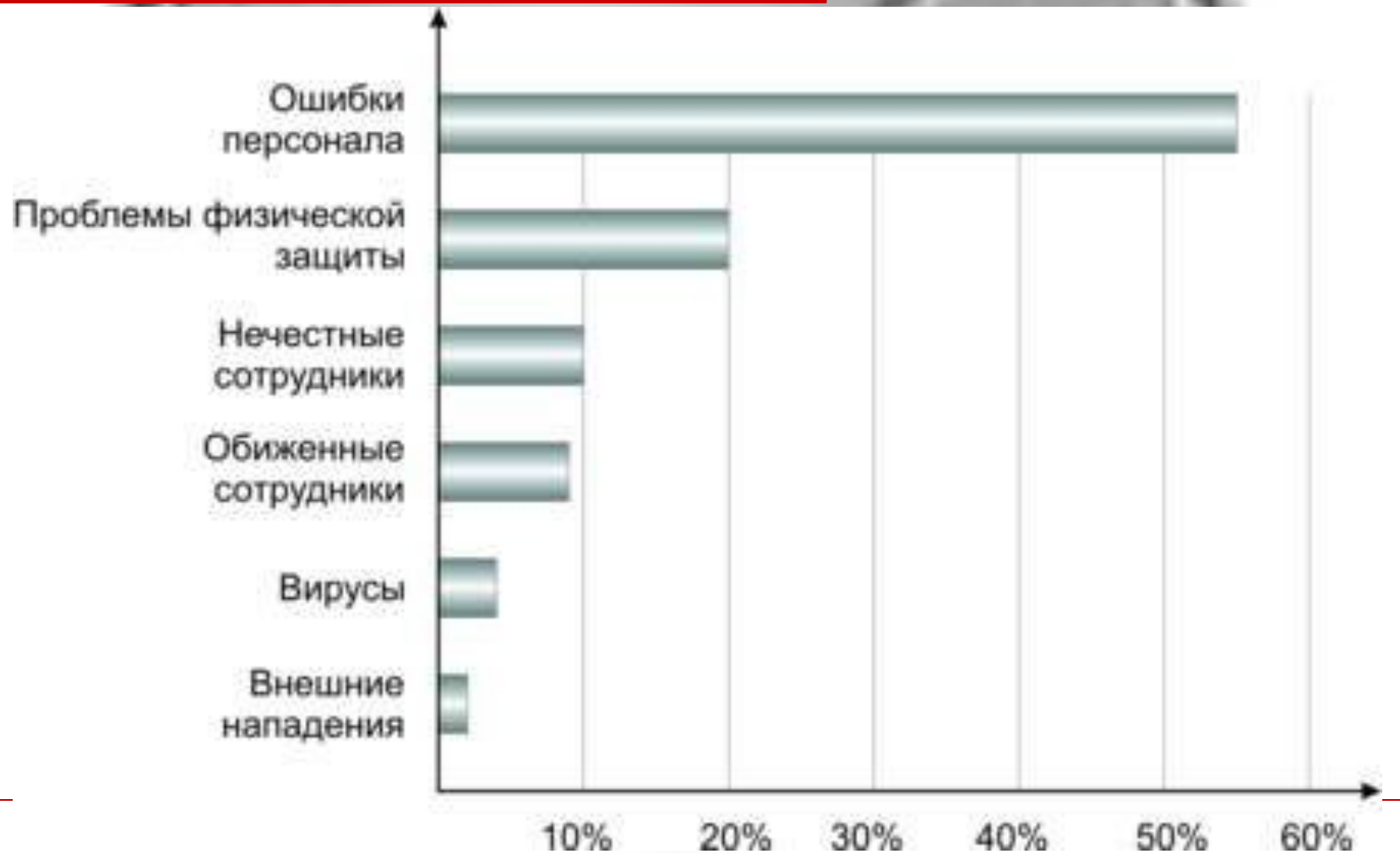
Внутренняя зона КС

Зона контролируемой территории

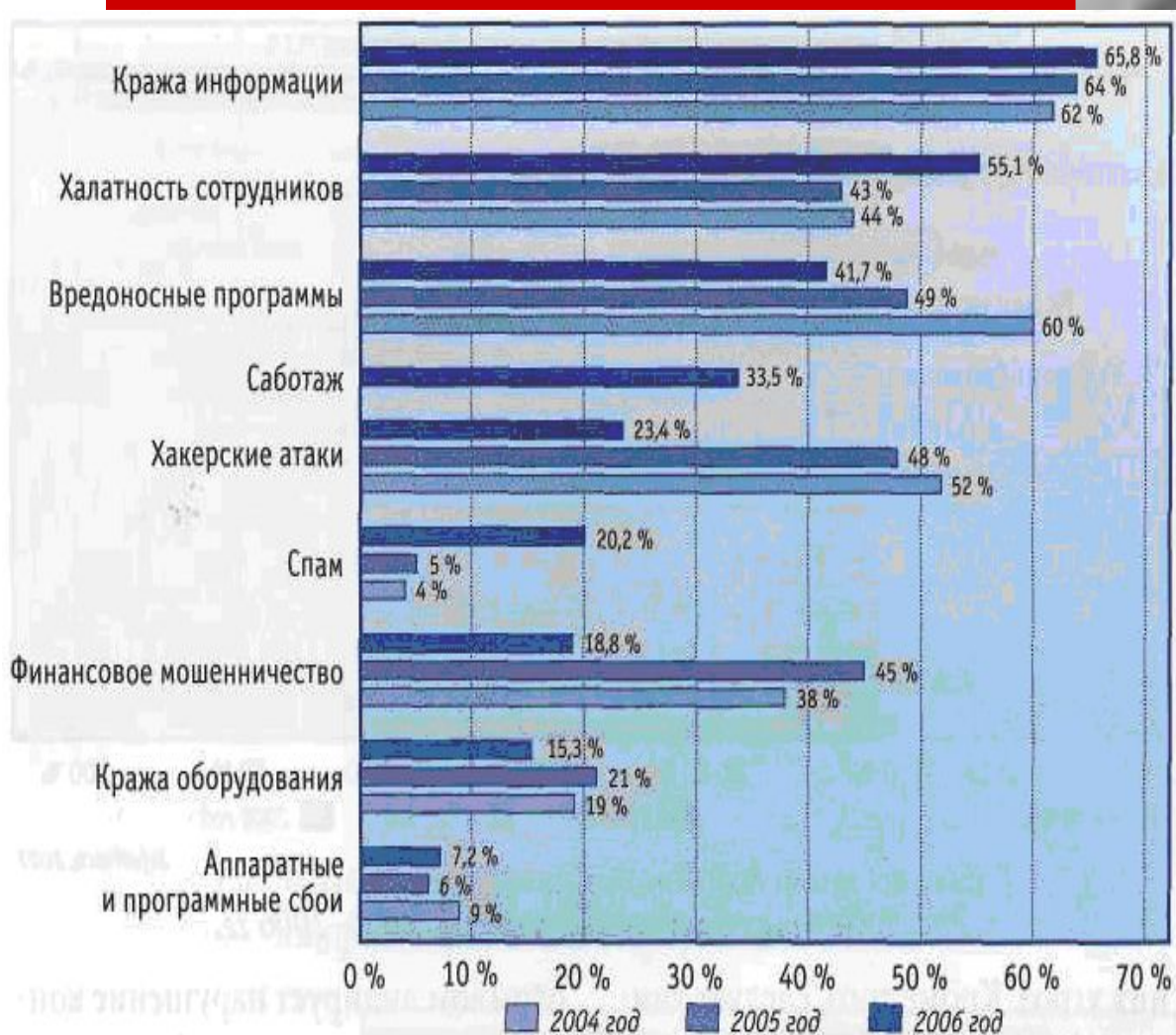
КС

Зона ресурсов КС

Соотношение угроз

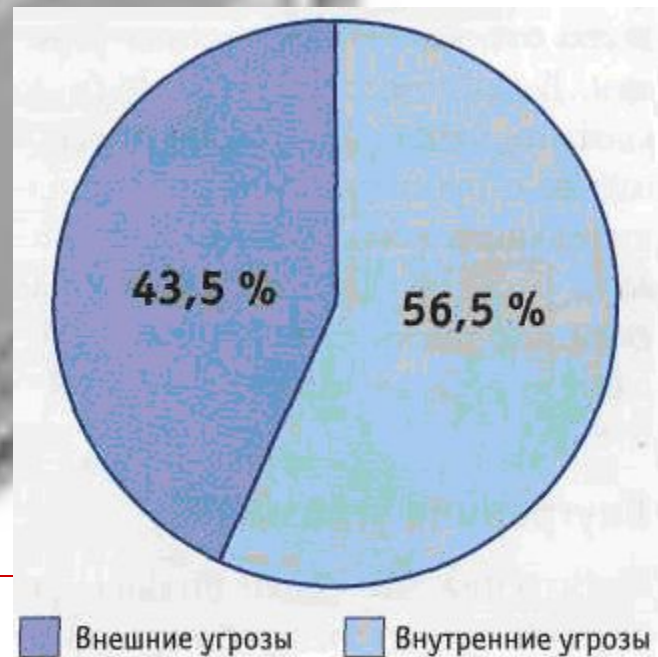


Соотношение некоторых видов угроз



InfoWatch, 2007

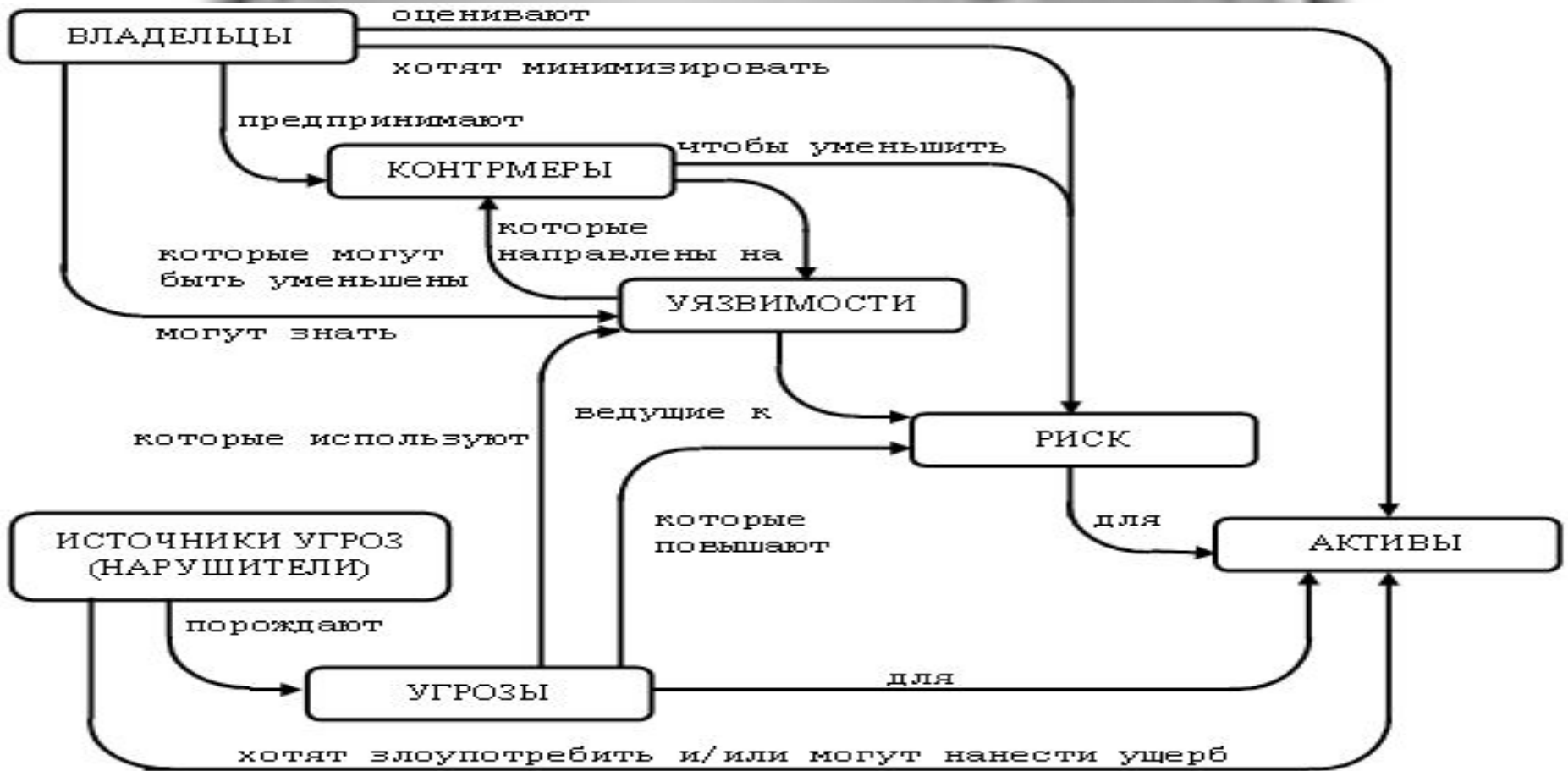
Соотношение внешних и внутренних (т.н. инсайдерских) угроз



Внешние угрозы Внутренние угрозы

InfoWatch, 2007

Понятия безопасности и их взаимосвязь



Процесс создания КС в аспекте обеспечения безопасности:

1. Идентификация и оценка защищаемых активов (*конфиденциальность, целостность, доступность*) и функций КС
2. **Идентификация угроз безопасности (выявление и спецификация - источники/ природа; активы/ функции, подвергаемые воздействию; методы/ способы/ особенности реализации; используемые уязвимости) и их оценка**
3. Выбор и обоснование функциональных требований к КС (архитектура и лежащие в ее основе модели обеспечения конфиденциальности/целостности/ доступности; функции обеспечения безопасности)
4. Реализация функциональных требований в процессе проектирования/создания
5. Оценка степени реализации функциональных требований (сертификация по требованиям безопасности), в т.ч. возможных уязвимостей, брешей безопасности

Каталоги (таксономические схемы классификации) угроз безопасности

- ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию.
<http://linux.nist.fss.ru>
- Bundesamt für Sicherheit der Informationstechnik (Германский стандарт безопасности ИТ), <http://www.bsi.de>
- РД ГосТехКомиссии России. Безопасность ИТ. Руководство по формированию семейств профилей защиты <http://www.fstec.ru>

Классы, подклассы и группы факторов (ГОСТ Р 51275-99)

Объективные

Внутренние

Передача сигналов по проводным линиям связи

Передача сигналов по оптико-волоконным линиям связи

Излучение сигналов, функционально-присущих ОИ

ПЭМИ

Паразитные электромагнитные излучения

Наводки

Акустозлектрические преобразования в элементах ТС ОИ

Дефекты, сбои, аварии ТС и систем ОИ

Дефекты, сбои и отказы программного обеспечения ОИ

Явления техногенного характера

Природные явления, стихийные бедствия

Внешние

Субъективные

Внутренние

Разглашение ЗИ лицами, имеющими к ней право доступа

Неправомерные действия со стороны лиц, имеющих право доступа к ЗИ

НСД к ЗИ (внутренний)

Неправильное организационное обеспечение ЗИ

Неправильное организационное обеспечение ЗИ

Ошибки обслуживающего персонала ОИ

Доступ к ЗИ с применением технических средств

НСД к ЗИ (внешний)

Блокирование доступа к ЗИ путем перегрузки технических средств обработки информации ложными заявками на ее обработку

Действия криминальных групп и отдельных преступных элементов

Каталог угроз по Германскому стандарту

T.1 Форс-мажор	<ul style="list-style-type: none"> T.1.1. Опасности персоналу (болезни, несчастные случаи, забастовки,...) T.1.2. Недостатки ИС T.1.3. Молниеопасность T.1.4. Пожары T.1.5. Затопления T.1.6. Возгорание, замыкание кабелей T.1.7. Недопустимые температуры и влажность T.1.8. Запыления, загрязнения T.1.9. Утрата данных из-за сильных магнитных полей T.1.10. Недостатки во внешних сетях
T.2. Организа- ционные дефекты и недостатки	<ul style="list-style-type: none"> T.2.1. Отсутствие или неэффективное управление, руководство (60 факторов)
T.3 Челове- ческие недостат- ки	<ul style="list-style-type: none"> T.3.1. Потеря конфиденциальности/целостности данных в результате ошибок ИТ-персонала T.3.2. Разрушение оборудования или данных в результате небрежности T.3.3. Несоблюдение (несогласие) мер ИТ-безопасности(45 факторов)
T.4. Техн. недостат- ки	<ul style="list-style-type: none"> T.4.1. Разрушение вследствие аварий энергоснабжения ... (42 фактора)
T.5. Предна- мерен- ные действия	<ul style="list-style-type: none"> T.5.1. Подделка, искажение, разрушение оборудования или принадлежностей T.5.2. Искажение данных или программ T.5.3. Безконтрольный (неавторизованный) вход в здания T.5.4. Кражи, хищения T.5.5. Вандализм T.5.6. Атаки T.5.7. Перехват с линий связи ... (99 факторов)

Методология объектов и угроз в продуктах и системах ИТ (РД ГосТехКомиссии «Руководство по разработке ПЗ и ЗБ, 2003г., пример)

- Угрозы данным на носителях
- Угрозы данным в телекоммуникационных линиях
- Угрозы прикладным программам (приложениям)
- Угрозы прикладным процессам и данным
- Угрозы отображаемым данным
- Угрозы вводимым данным
- Угрозы данным, выводимым на печать
- Угрозы данным пользователей
- Угрозы системным службам и данным
- Угрозы информационному оборудованию

Аспекты угрозы

- источник угрозы (люди либо иные факторы)
- предполагаемый метод (способ, особенности) нападения/реализации
 - уязвимости, которые м.б. использованы для нападения/реализации
- активы, подверженные нападению/реализации

Методология объектов и угроз в продуктах и системах ИТ (РД ГосТехКомиссии «Руководство по разработке ПЗ и ЗБ, 2003г., пример)

Данные на носителях

данные раскрыты путем незаконного перемещения носителя

обращение к данным, изменение, удаление, добавление в приложение или извлечение из приложения данных неуполномоченным лицом

данные раскрыты путем их выгрузки с носителя данных неуполномоченным лицом

использование остаточной информации на носителе

незаконное копирование данных

данные незаконно используются, или их использование затруднено из-за изменения атрибутов доступа к данным неуполномоченным лицом

данные получены незаконно путем фальсификации файла

данные повреждены из-за разрушения носителя

данные уничтожены или их использование затруднено из-за неисправности устройства ввода-вывода

обращение к данным, изменение, удаление, добавление в приложение или извлечение из приложения данных неуполномоченным лицом путем использования соответствующей команды

зашифрованные данные не могут быть дешифрованы из-за потери секретного ключа

Методология объектов и угроз в продуктах и системах ИТ (РД ГосТехКомиссии «Руководство по разработке ПЗ и ЗБ, 2003г., пример)

Данные в телекоммуникациях

данные перехвачены или разрушены в телекоммуникационной линии

данные прослушиваются, незаконно умышленно изменены, искажены, похищены, удалены или дополнены в системе коммутации

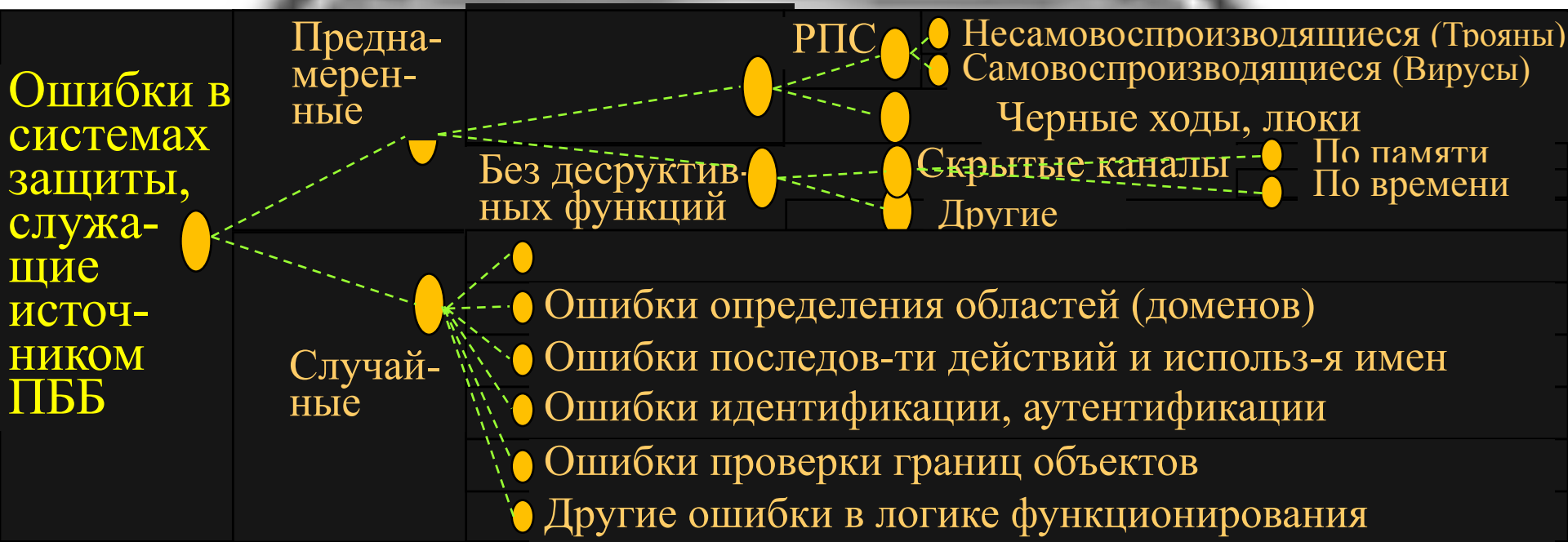
данные незаконно используются в результате подмены их адресата, отправителя или изменения атрибутов доступа в системе коммутации

связь заблокирована из-за повреждения линии

связь заблокирована из-за аномалий в канале связи

И т.д.

Потенциальные бреши безопасности (ППБ)



Ошибки на этапах внедрения, вызывающие ПББ	На стадии разработки	Ошибки в требованиях и спецификациях	22
		Ошибки в исходных текстах программ	15
		Ошибки в исполняемом коде	1
	В ходе сопровождения	В ходе эксплуатации	9
		В ходе эксплуатации	3

Потенциальные бреши безопасности

ППБ по месту размещения в КС	Программное обеспечение	Операционные системы	● Инициализация ОС (загрузка)	8	
			● Управление выделением памяти	2	
			● Управление процессами	10	
			- Управление устройствами	3	
	Прикладные программы		● Средства идент-ии и аутентификации	6	
			● Другие (неизвестные)	5	
			● Привилегированные утилиты	1	
			● Непривилегированные утилиты	10	
	Аппаратное обеспечение		Прикладные программы		3
			Аппаратное обеспечение		3

Примеры угроз доступности

- *непреднамеренные ошибки штатных пользователей, обслуживающих ИС – 65%*
 - *Максимальная автоматизация*
 - *отказ пользователей -нет желания, нет знаний, нет документации ;*
 - *внутренний отказ информационной системы –*
 - *отступление (случайное или умышленное) от установленных правил эксплуатации;*
 - *выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);*
 - *ошибки при (пере)конфигурировании системы;*
 - *отказы программного и аппаратного обеспечения;*
 - *разрушение данных;*
 - *разрушение или повреждение аппаратуры.;*
 - *отказ поддерживающей инфраструктуры.*
 - *нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;*
 - *разрушение или повреждение помещений;*
 - *невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).*
 - *Обиженные сотрудники*
 - *Стихийные бедствия – 13%*
-

Вредоносное ПО

- Грани вредоносного ПО:
 1. вредоносная функция;
 - внедрение другого *вредоносного ПО* ;
 - получение контроля над *атакуемой* системой;
 - *агрессивное потребление ресурсов* ;
 - изменения или разрушения программ и/или данных.
 - И т.д.
 2. способ распространения;
 3. *внешнее представление.*
 - Программный *вирус* - это исполняемый или интерпретируемый программный код, обладающий свойством
 - несанкционированного распространения и
 - самовоспроизведения в автоматизированных системах или *телекоммуникационных сетях*
 - (2) Вирусы, Черви, Троянские программы, Мобильные агенты
-

Пример угроз целостности

- Кражи и подлоги (нечестные сотрудники)
 - Нарушение статической целостности
 - Ввод неверных данных, изменение данных, отказ от совершенных действий
 - Нарушение динамической целостности
 - нарушение атомарности транзакций, переупорядочение, *кража, дублирование данных* или внесение дополнительных сообщений (сетевых пакетов и т.п.).
 - Соответствующие действия в сетевой среде - активное прослушивание.
-

Пример угроз конфиденциальности

- Конфиденциальная информация - предметная и служебная (пароли)
 - Изначально порочный принцип парольной защиты
 - *угрозы* конфиденциальности могут носить некомпьютерный и нетехнический характер (пароли в записных книжках)
 - размещение конфиденциальных данных в среде, где им не обеспечена необходимая защита (разговоры по телефону, выставки, резервное копирование) – перехват данных техническими средствами
 - *методы морально-психологического воздействия, фишинг*
 - ***злоупотребление полномочиями, администраторы***
-

Успех может принести только *комплексный* подход к ЗИ

- Для защиты интересов субъектов *информационных отношений* необходимо сочетать меры следующих уровней:
 - законодательного;
 - административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
 - процедурного (меры безопасности, ориентированные на людей);
 - программно-технического.
-