Защиты базы данных от несанкционированного доступа

Базы данных, которые являются мировыми ресурсами, то есть используются в мировой сети, имеют приоритет международных. Доступ в такие базы данных может быть ограничен.

Для этого создается специальный модуль, который является основным инструментом защиты базы данных от несанкционированного доступа и предназначен для настройки, включения и отключения системы разграничения прав доступа пользователей к базе данных.

Система разграничения прав доступа должна выполнять следующие функции:

- блокировать доступ незарегистрированных пользователей в систему. С этой целью все пользователи системы должны быть зарегистрированы в списке пользователей;
- определять права пользователей в системе и ограничивать действия пользователей в соответствии с этими правами: права на доступ к базе данных и права на пользование рабочими станциями;

- вести журнал регистрации системных событий, в котором регистрируются дата, время, имя пользователя, совершившего действие: вход/выход из системы, неудачный вход, запуск интерфейсов, запуск отчетов, запуск процессов.

Базы данных могут классифицироваться по отраслям, по видам деятельности, по направлениям и так далее. В этом случае они приобретают статус специализированных баз данных, и напоминают собой всем известные тематические энциклопедии.

В настоящее время особое внимание уделяется защите баз данных, как и других информационных технологий, от пиратского копирования. В общем случае система защиты от несанкционированного копирования представляет собой комплекс средств, предназначенный для затруднения (в идеале – предотвращения) нелегального копирования (исполнения) защищаемого программного модуля, с которым она ассоциирована.

Обобщенные сведения из различных источников позволяют предложить следующую структуру системы защиты от несанкционированного копирования (см. рис. 1).

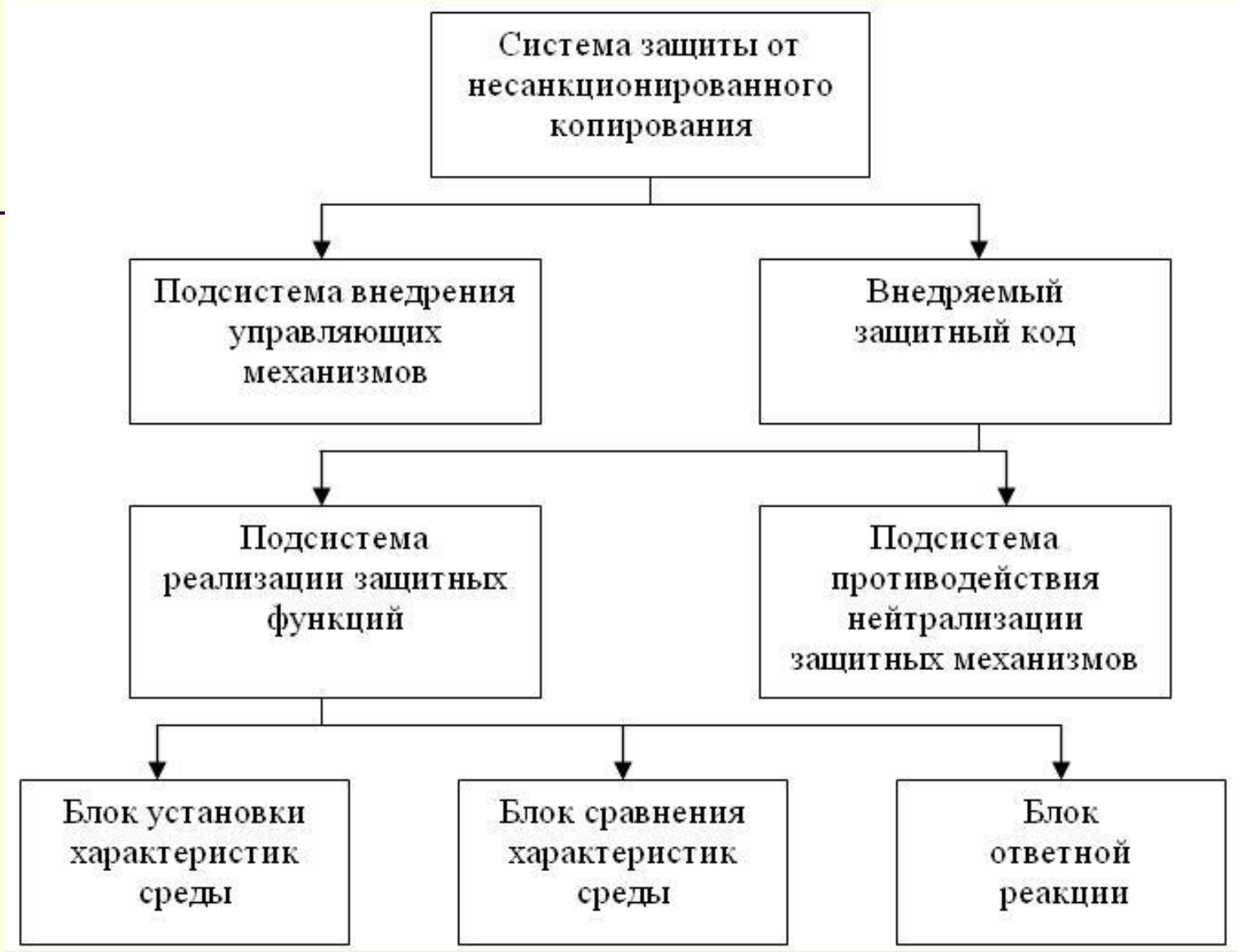


Рис.1. Структура системы защиты от несанкционированного копирования

Подсистема внедрения управляющих механизмов представляет собой комплекс программных средств, предназначенный для подключения внедряемого защитного кода к защищаемому программному модулю.
Внедряемый защитный код – это программный модуль, задача которого состоит в противодействии попыткам запуска (исполнения) нелегальной копии защищаемой программы.

Подсистема реализации защитных функций представляет собой программную секцию, решающую задачу распознавания легальности запуска защищаемой программы.

Подсистема противодействия нейтрализации защитных механизмов предназначена для борьбы с возможными попытками нейтрализации системы защиты от несанкционированного копирования и/или её дискредитации.

Блок установки характеристик среды отвечает за получение характеристик, идентифицирующих вычислительную среду.

Блок сравнения характеристик среды устанавливает факт легальности запуска защищаемой программы.

Блок ответной реакции реализует ответные действия системы защиты на попытки несанкционированного исполнения защищаемой программы.

Долгое время защита баз данных ассоциировалась с защитой локальной сети предприятия от внешних атак хакеров, вирусов и т.п. Данные консалтинговых компаний, появившиеся в последние годы, выявили другие, не менее важные направления защиты информационных ресурсов компаний.

Исследования убедили, что от утечки информации, ошибок персонала и злонамеренных действий “всесильных” администраторов баз данных не спасают ни межсетевые экраны, ни VPN, ни даже “навороченные” системы обнаружения атак и анализа защищенности. Обратимся к свидетельствам, опубликованным в конце 2004г. на известном российскому ИТ-сообществу сайте www.CNews.ru (рис.1) .

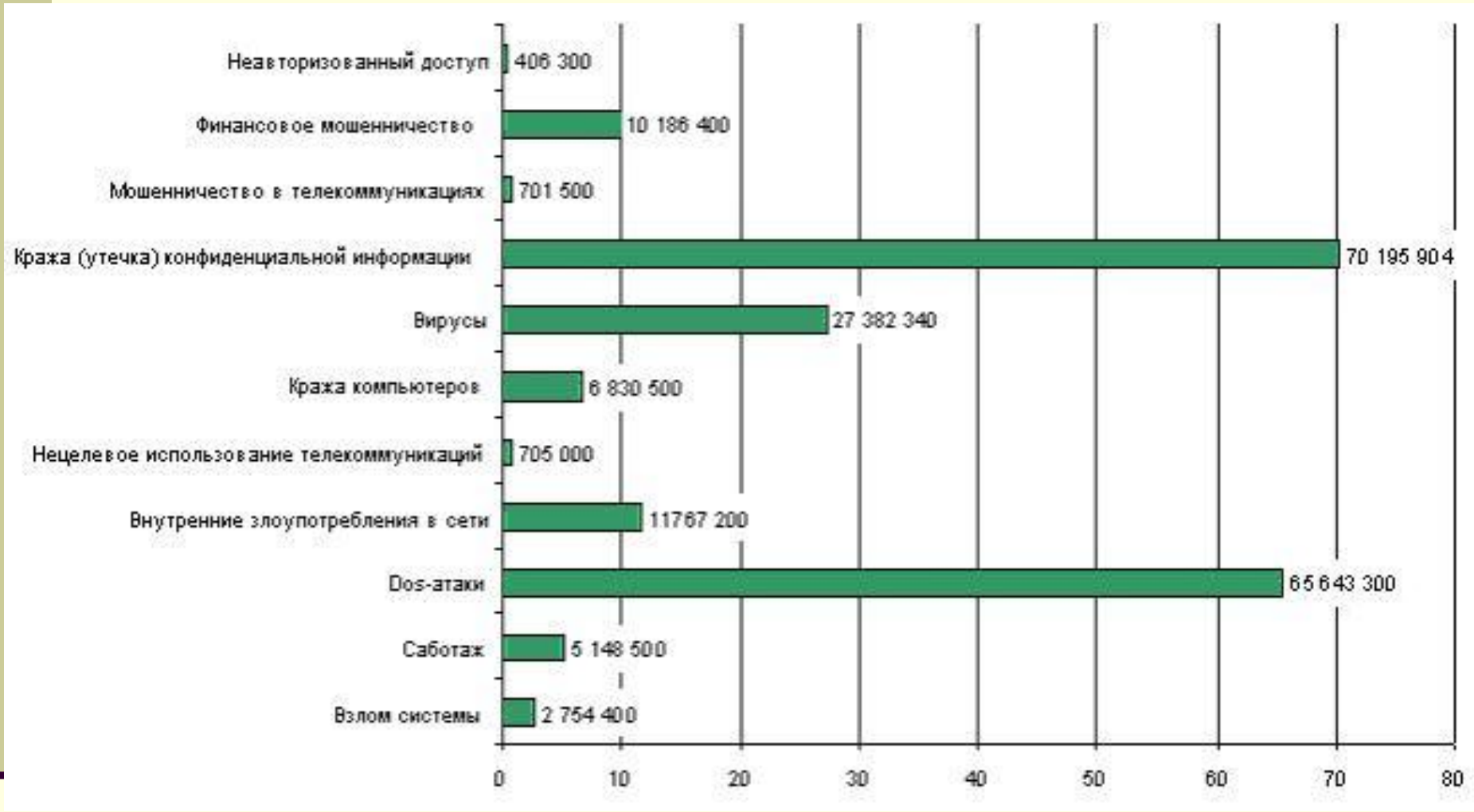


Рис. 1.Статистика угроз.
Источник: 2003 CSI/FBI Computer Crime and Security Survey, данные по 1000 исследуемых компаний

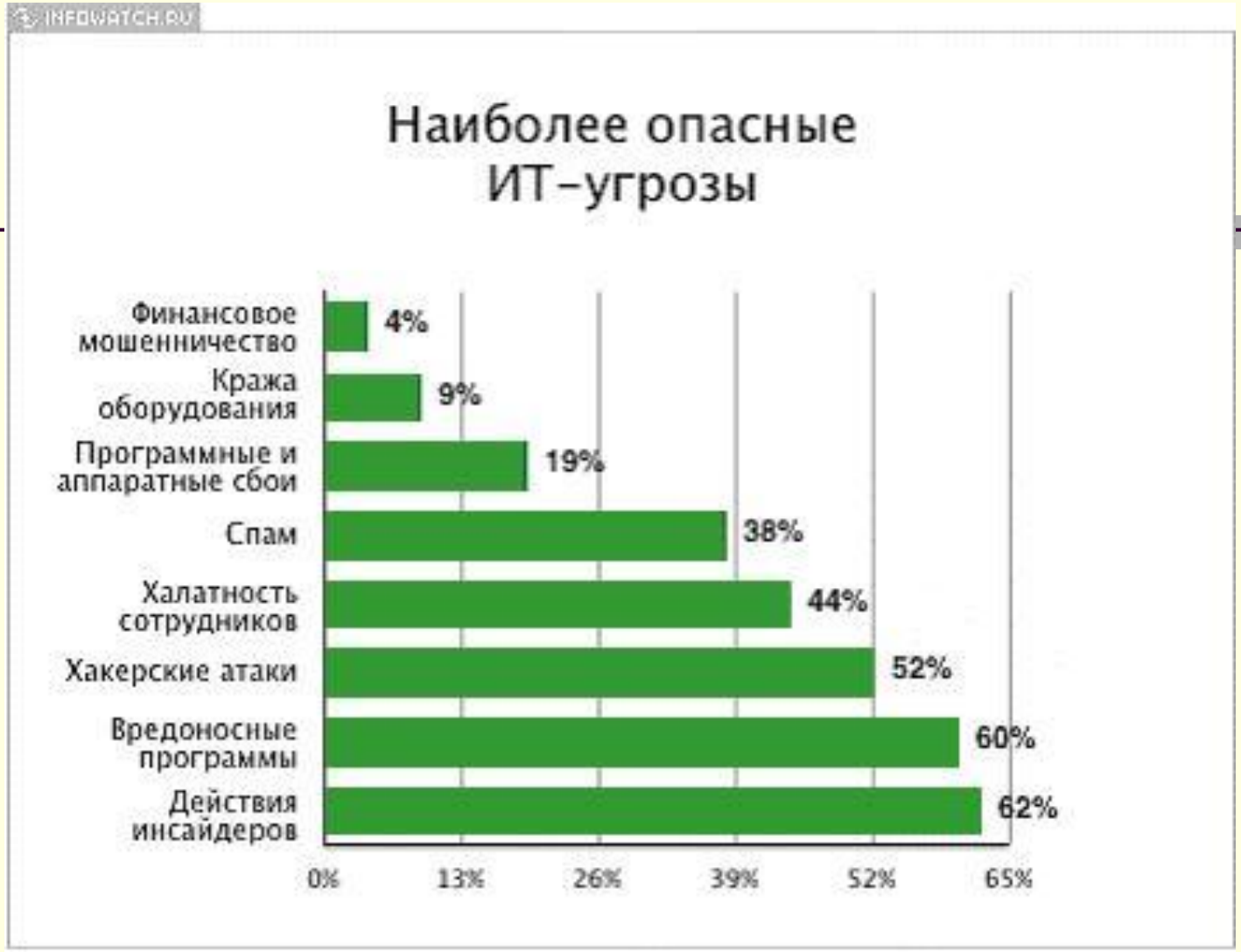
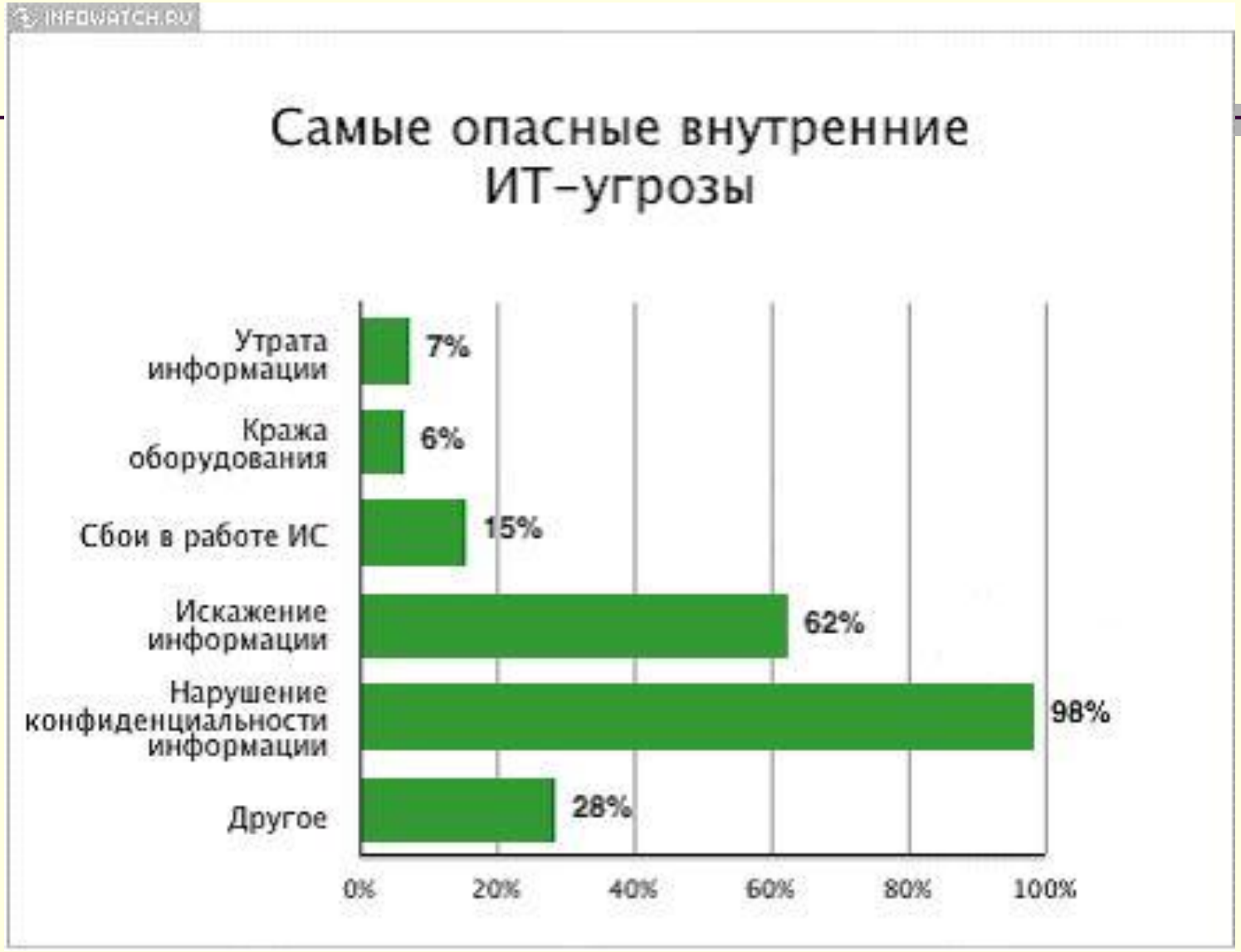


Рис. 2. Оценка угроз. Данные компании Infowatch октябрь-декабрь 2004 г.


INFOWATCH.RU
Самые опасные внутренние ИТ-угрозы
Утрата информации
7%
Кража оборудования
6%
Сбои в работе ИС
15%
Искажение информации
62%
Нарушение конфиденциальности информации
98%
Другое
28%
0%
20%
40%
60%
80%
100%