МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Сергеев Александр Иванович

Основная литература

1 Грибунин, В. Г. Комплексная система защиты информации на пред-приятии : учеб. пособие для вузов / В. Г. Грибунин, В. В. Чудовский . - М. : Ака-демия, 2009. - 413 с.

2 Мельников, В. П. Информационная безопасность и защита информа-ции : учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петра-ков; под ред. С. А. Клейменова.- 4-е изд., стер. - М. : Академия, 2009. - 332 с.

3 Основы защиты компьютерной информации : учеб. пособие для вузов / А. И. Сердюк [и др.] ; М-во образования и науки Рос. Федерации, Федер. агент-ство по образованию, Гос. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т". - Оренбург : ГОУ ОГУ, 2009. - 200 с. : ил..

4 Шаньгин, В. Защита компьютерной информации. Эффективные ме-тоды и средства / В. Шаньгин. – М. : ДМК, 2008. – 544 с.

Журналы

1 Хакер
2 Компьютер-Пресс
3 Мир ПК

Дополнительная литература

1 Бернет, С. Криптография. Официальное руководство RSA Security = RSA Security's Official Guide to Cryptography / С. Бернет, С. Пэйн ; пер. с англ. под ред. А. И. Тихонова. - М. : Бином, 2009. - 382 с. : ил.

2 Завгородний, В. И. Комплексная защита информации в компьютер-ных системах: Учеб. пособие для вузов / В. И. Завгородний. - М. : Логос, 2001. - 264с. : ил. - (Учеб. 21 в.). - Библиогр. : с. 260 - 263.

.3 Скиба, В. Ю. Руководство по защите от внутренних угроз информа-ционной безопасности / В. Ю. Скиба, В. А. Курбатов. – СПб. : Питер, 2008. – 320 с. : ил.

4 Торокин, А. А. Инженерно-техническая защита информации / А. А. Торокин. – М. : Гелиос АРВ, 2005. – 960 с.

5 Хорев, П. Б. Методы и средства защиты информации в компьютер-ных системах / П. Б.Хорев. – М. : Академия, 2007. – 256 с.

6 ГОСТ 28147 – 89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

7 ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

8 ГОСТ 2.511-2011 ЕСКД. Правила передачи электронных конструкторских документов. Общие положения

9 ГОСТ 2.512-2011 ЕСКД. Правила выполнения пакета данных для передачи электронных конструкторских документов. Общие положения

Интернет-ресурсы

1 Журнал «САПР и графика». – Режим доступа: http://www.sapr.ru.

2 САПР CAD/CAM/CAE - Системы Черчение 3D Моделирование. – Режим доступа: http://rucadcam.ru.

3 Все о САПР, PLM и ERP. – Режим доступа: http://isicad.ru.

4 Издательство «Открытые системы». – Режим доступа: http://www.osp.ru.

5 Профессиональные программы для разработчиков: Delphi World, Web Development Studio. – Режим доступа: http://delphiworld.narod.ru.

6 Директор по безопасности. – Режим доступа: http://www.s-director.ru.

После изучения курса Вы будете иметь представление:

- о современных сетевых средствах и методах обработки информации
- об основных рисках и формах атак на информацию, а так же способах защиты от них
- о современных программах защиты информации, а также программах обеспечивающих доступ к защищенной информации

будете знать:

- методы криптографической защиты информации
- методы и средства борьбы с компьютерными вирусами
- особенности защиты информации в распределенных компьютерных системах

будете уметь:

- создавать приложения, позволяющие зашифровывать информацию по различным алгоритмам
- строить комплексные системы защиты информации

будете иметь навыки:

- работы с основными пакетами разработки приложений и пакетами защиты информации, принятыми в ГОУ ОГУ

Лекция **1 –** Введение в информационную безопасность при работе в автоматизированных системах

Рассматриваемые вопросы:

1) **современная ситуация в области информационной безопасности;**
2) **основные определения в области защиты информации;**
3) **категории информационной безопасности;**
4) **абстрактные модели защиты информации.**

Вопрос **1 -** Современная ситуация в области информационной безопасности

В современном обществе именно **информация** становится **важнейшим стратегическим ресурсом**, основной производительной силой, обеспечивающей его дальнейшее развитие. Поэтому, подобно другим традиционно существующим ресурсам, информация нуждается в своей сохранности и защите.

Защитить информацию – это значит:

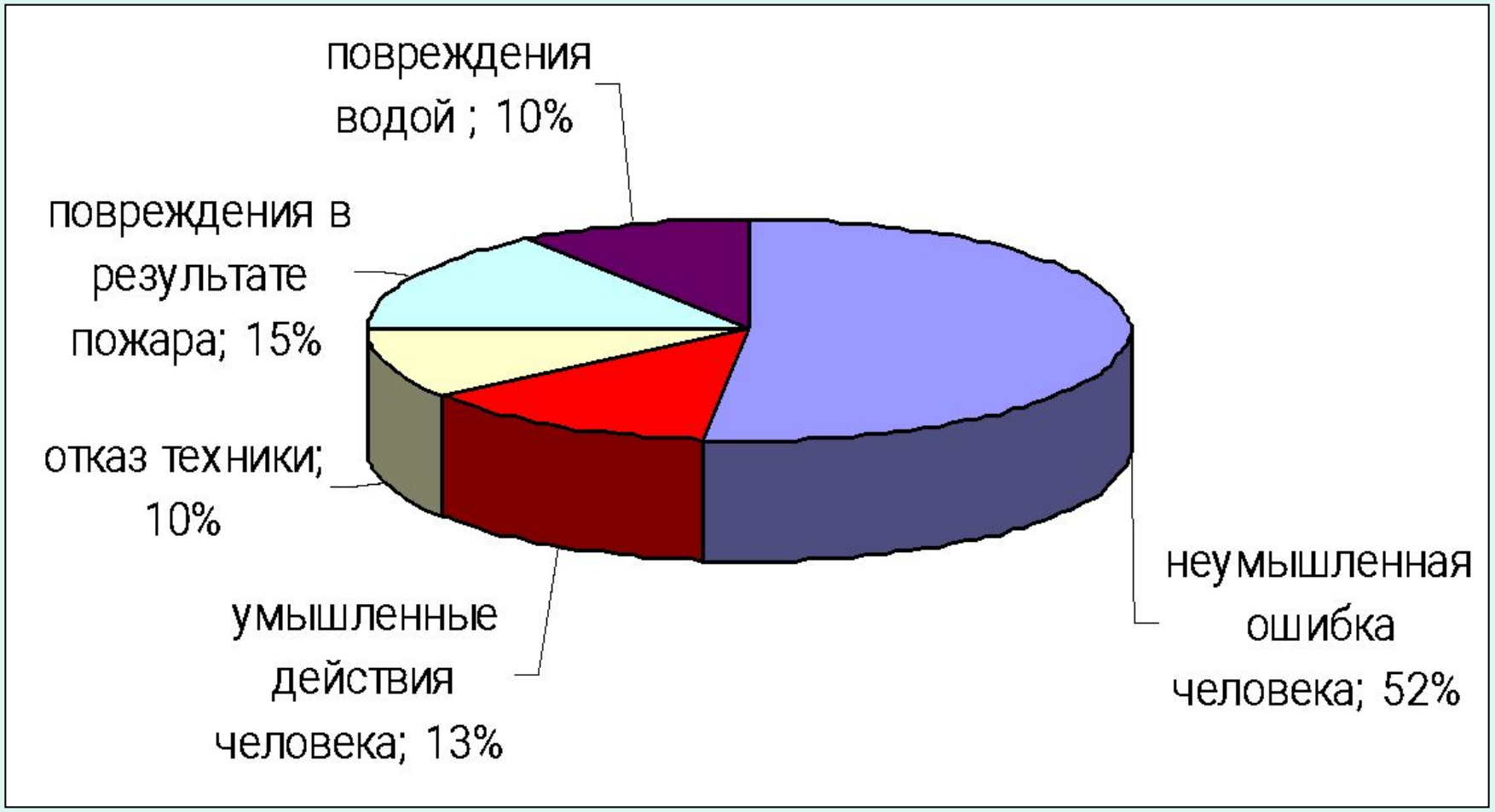
- обеспечить ее физическую целостность, т.е. не допустить искажения или уничтожения элементов информации;

- не допустить подмены (модификации) элементов информации при сохранении ее целостности;

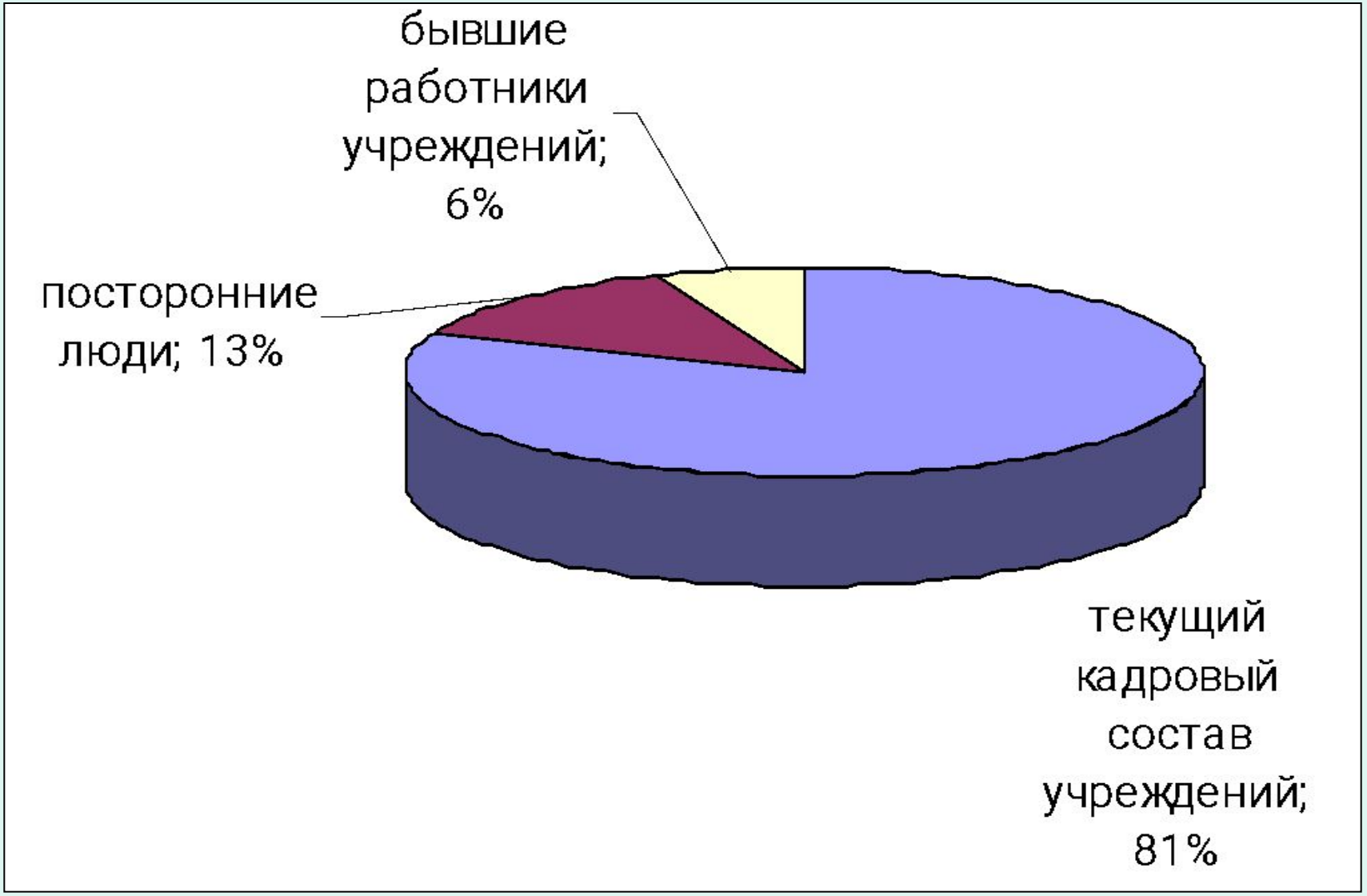
- не допустить несанкционированного получения информации лицами или процессами, не имеющими на это соответствующих полномочий;

- быть уверенным в том, что передаваемые (продаваемые) владельцем информации ресурсы будут использоваться только в соответствии с обговоренными сторонами условиями.

Основные причины повреждений электронной информации по данным исследовательского центра DataPro Research

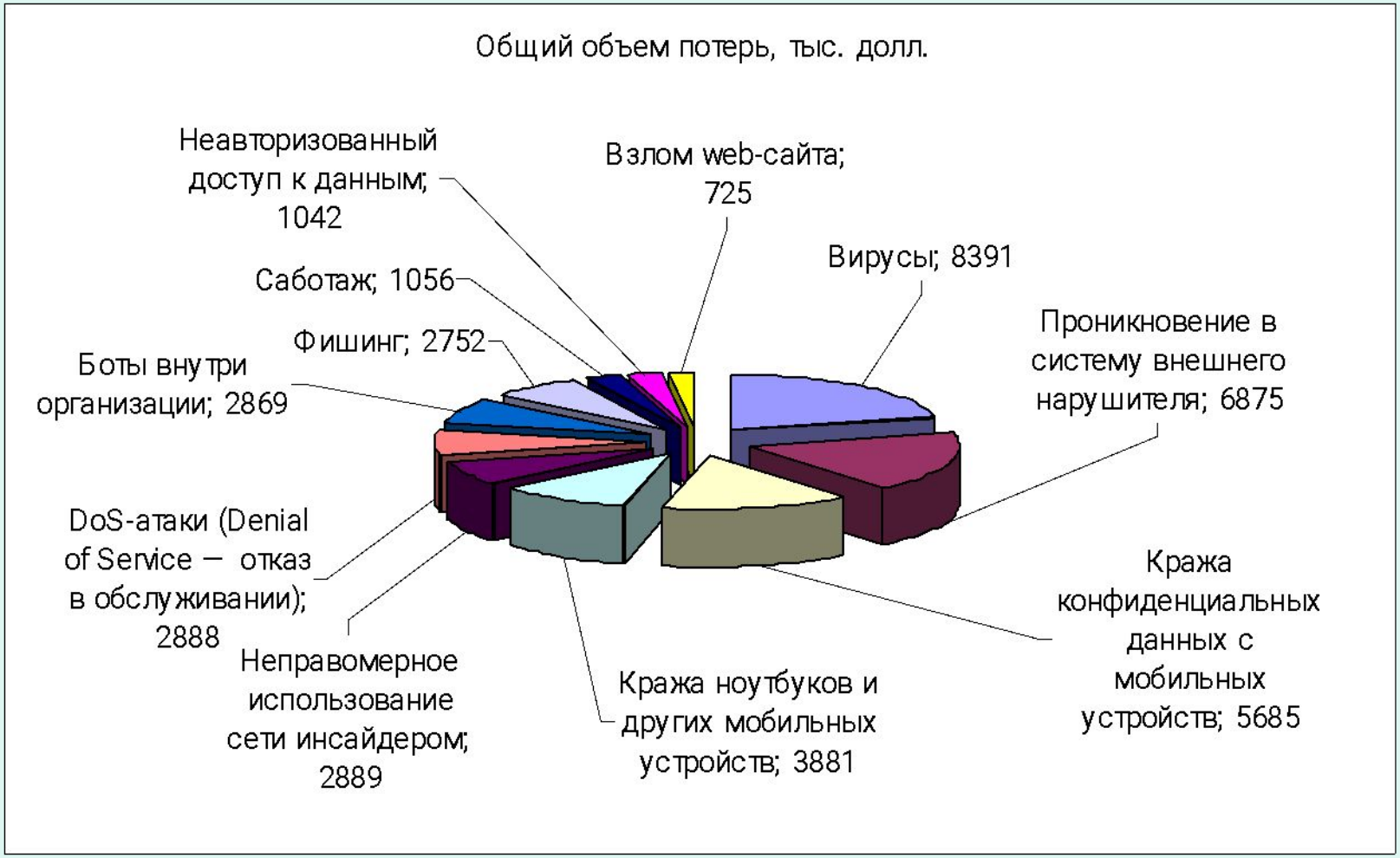


Кто совершает повреждения электронных данных ?



Действия злоумышленников при получении доступа к конфиденциальной информации

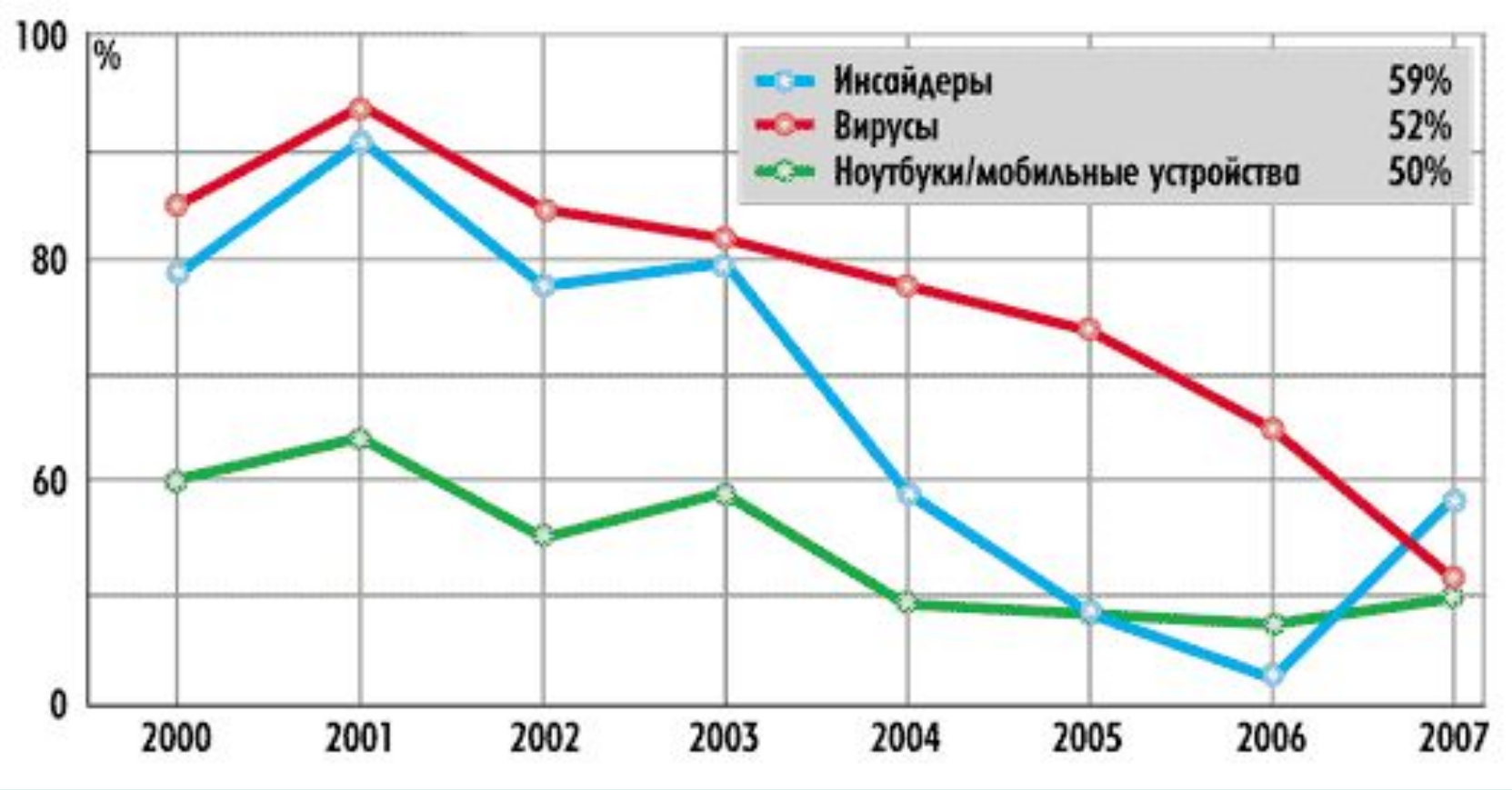
Десятка ИТ-угроз, которые привели к наибольшим финансовым потерям, США (источник: CSI, 2007)



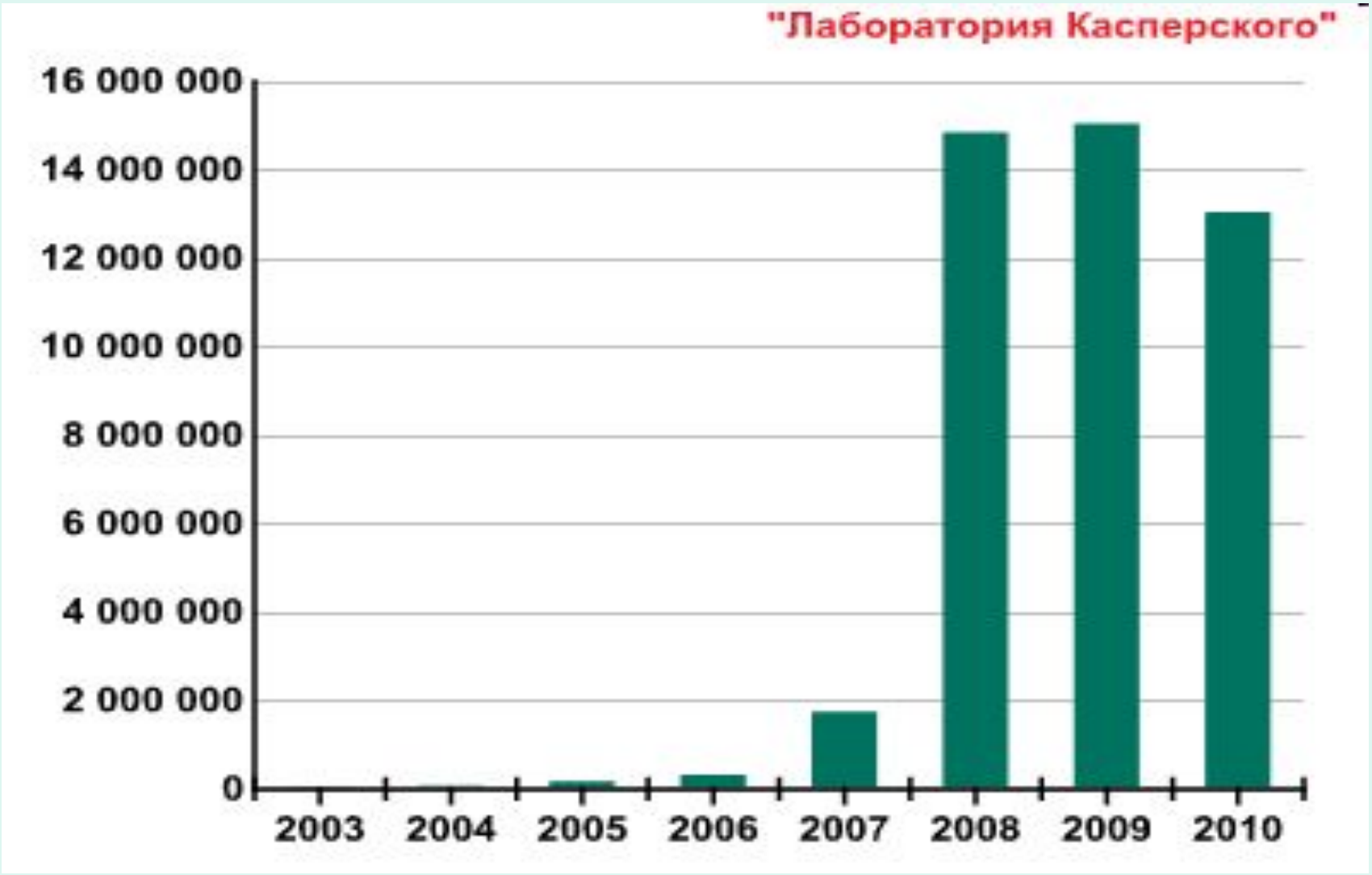
Десятка ИТ-угроз, которые привели к наибольшим финансовым потерям, США (источник: CSI, 2007)

Позиция в рейтинге	ИТ-угроза
1	Угроза инсайдеров
2	Спам
3	Malware-угрозы (компьютерные вирусы, черви, троянцы, adware- и spyware-модули)
4	Неавторизованный доступ со стороны внешних нарушителей
5	Угроза физической потери носителя информации
6	Электронное мошенничество
7	Pharming-атаки
8	Phishing-атаки
9	Электронный вандализм и саботаж
10	DoS-атаки

Динамика развития основных типов ИТ-атак в 2000-2007 годах (источник: CSI, 2007)



Число новых вредоносных программ, добавляемых в коллекцию «Лаборатории Касперского»



Распределение по странам компьютеров, на которых были зафиксированы локальные заражения

Место	Страна*	% уникальных попыток заражения**
1	Китай	19,86%
2	Россия	15,53%
3	Индия	7,35%
4	США	5,72%
5	Вьетнам	4,44%
6	Украина	2,59%
7	Германия	2,36%
8	Мексика	2,18%
9	Италия	2,08%
10	Малайзия	2,07%
11	Франция	2,00%
12	Саудовская Аравия	1,92%
13	Турция	1,91%
14	Испания	1,88%
15	Бразилия	1,77%
16	Великобритания	1,67%
17	Египет	1,66%
18	Таиланд	1,58%
19	Польша	1,26%
20	Индонезия	1,12%

Затраты, связанные с наиболее распространенными инсайдерскими преступлениями в России (источник: PricewaterhouseCoopers, 2007)

Текущее и идеальное распределение времени специалистов по приватности данных

Вопрос **2 -** Основные определения в области защиты информации

- **БЕЗОПАСНОСТЬ ИНФОРМАЦИИ** – состояние защищенности информации, хранимой и обрабатываемой в автоматизированной системе, от негативного воздействия на нее с точки зрения нарушения ее физической и логической целостности (уничтожения, искажения) или несанкционированного использования.

- **УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ** – события или действия, которые могут вызвать нарушение функционирования автоматизированной системы, связанное с уничтожением или несанкционированным использованием обрабатываемой в ней информации.

- **ЗАЩИЩЕННОСТЬ ИНФОРМАЦИИ** – поддержание на заданном уровне тех параметров находящейся в автоматизированной системе информации, которые характеризуют установленный статус ее хранения, обработки и использования.

Защита информации - процесс создания и использования в автоматизированных системах специальных механизмов, поддерживающих установленный статус ее защищенности.

Защита информации от утечки:

деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

Защита информации от непреднамеренного воздействия:

деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от несанкционированного воздействия:

деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

- **УЯЗВИМОСТЬ ИНФОРМАЦИИ** – возможность возникновения на каком-либо этапе жизненного цикла автоматизированной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

- **АВТОМАТИЗИРОВАННАЯ СИСТЕМА** – организованная совокупность средств, методов и мероприятий, используемых для регулярной обработки информации в процессе решения определенного круга прикладных задач.

- **АТАКА НА ИНФОРМАЦИЮ** – это умышленное нарушение правил работы с информацией. При хранении, поддержании и предоставлении доступа к любому информационному объекту его владелец, либо уполномоченное им лицо, накладывает явно либо самоочевидно набор правил по работе с ней. Умышленное их нарушение классифицируется как атака на информацию.

Вопрос **3 -** Категории информационной безопасности

Информация с точки зрения информационной безопасности обладает следующими категориями:

· **конфиденциальность** – гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется хищением либо раскрытием информации

· **целостность** – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения

· **аутентичность** – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется фальсификацией, но уже автора сообщения

· **апеллируемость** – гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой;

Категории информационной безопасности в отношении информационных систем:

· **надежность** – гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано

· **точность** – гарантия точного и полного выполнения всех команд

· **контроль доступа** – гарантия того, что различные группы лиц имеют различный доступ к информационным объектам, и эти ограничения доступа постоянно выполняются

· **контролируемость** – гарантия того, что в любой момент может быть произведена полноценная проверка любого компонента программного комплекса

· **контроль идентификации** – гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает

· **устойчивость к умышленным сбоям** – гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как оговорено заранее.

Вопрос **4 -** Абстрактные модели защиты информации

1) модель защиты информации **Биба (Biba)** – 1977 г.

2) модель защиты информации **Гогена-Мезигера (Goguen-Meseguer)** - 1982 г.

3) **Сазерлендская** (от англ. Sutherland) модель защиты информации - 1986 г .

4) модель защиты информации **Кларка-Вильсона** (Clark-Wilson) - 1987 г.

5) другие…