

A world map is shown in the background, overlaid with several vertical bands of color. From left to right, the bands are: red, orange, purple, cyan, blue, and dark blue. The map is rendered in a light, almost white color against a dark background.

Защита информации

Петелин Александр Евгеньевич

Роль информации в современном мире



ПРОИЗВОДСТВЕННЫЕ ПРОЦЕССЫ

Материальная
составляющая

Нематериальная
составляющая

Оборудование,
материалы,
энергия

Технология
производства

Себестоимость = стоимость [материалы, энергия,
рабочая сила] + стоимость [технология]



Утрата информации влечет:

- 1 Материальный ущерб**
- 2 Вмешательство в управление**

Защита информации – меры для

- 1 *ограничения доступа к информации для каких-либо лиц (категорий лиц)***
- 2 *удостоверения подлинности и неизменности информации***

Аспекты защиты



**перед защитой
необходимо
определить
перечень
вероятных угроз**

**хорошая
защита
обходится
дорого, плохая
никому не нужна**

**большое значение
имеет не только
объективная
надёжность
защиты, но и
отношение к защите
других людей**



Безопасность информации

(information security) — такое состояние защищаемой информации в системе обработки, когда её несанкционированное получение лицами и процессами, не имеющими на это специальных полномочий, становится невозможным или сводится к уровню не выше допустимого.

Понятие безопасности

информации тесно связано с понятиями «безопасность данных» и «защита данных».



Безопасность данных (data security) — это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное или преднамеренное получение, изменение или уничтожение.

Защита данных —

совокупность целенаправленных действий и мероприятий по обеспечению безопасности данных.

Таким образом, защита данных есть процесс обеспечения безопасности данных, а безопасность — состояние данных, конечный результат процесса защиты.



Безопасность человеческого общества складывается из:

- 1) ядерной безопасности;
- 2) технологической безопасности;
- 3) экономической безопасности;
- 4) политической безопасности;
- 5) информационной безопасности.



Информационная

безопасность — это

состояние защищенности

информационной среды общества,

обеспечивающее ее формирование и

развитие в интересах граждан,

организаций и государства.



Информационная безопасность

Информационная безопасность
отдельно взятого человека, коллективов
людей и общества

= Защита от дезинформации,
информационного прессинга,
информационного зомбирования и
т.д.

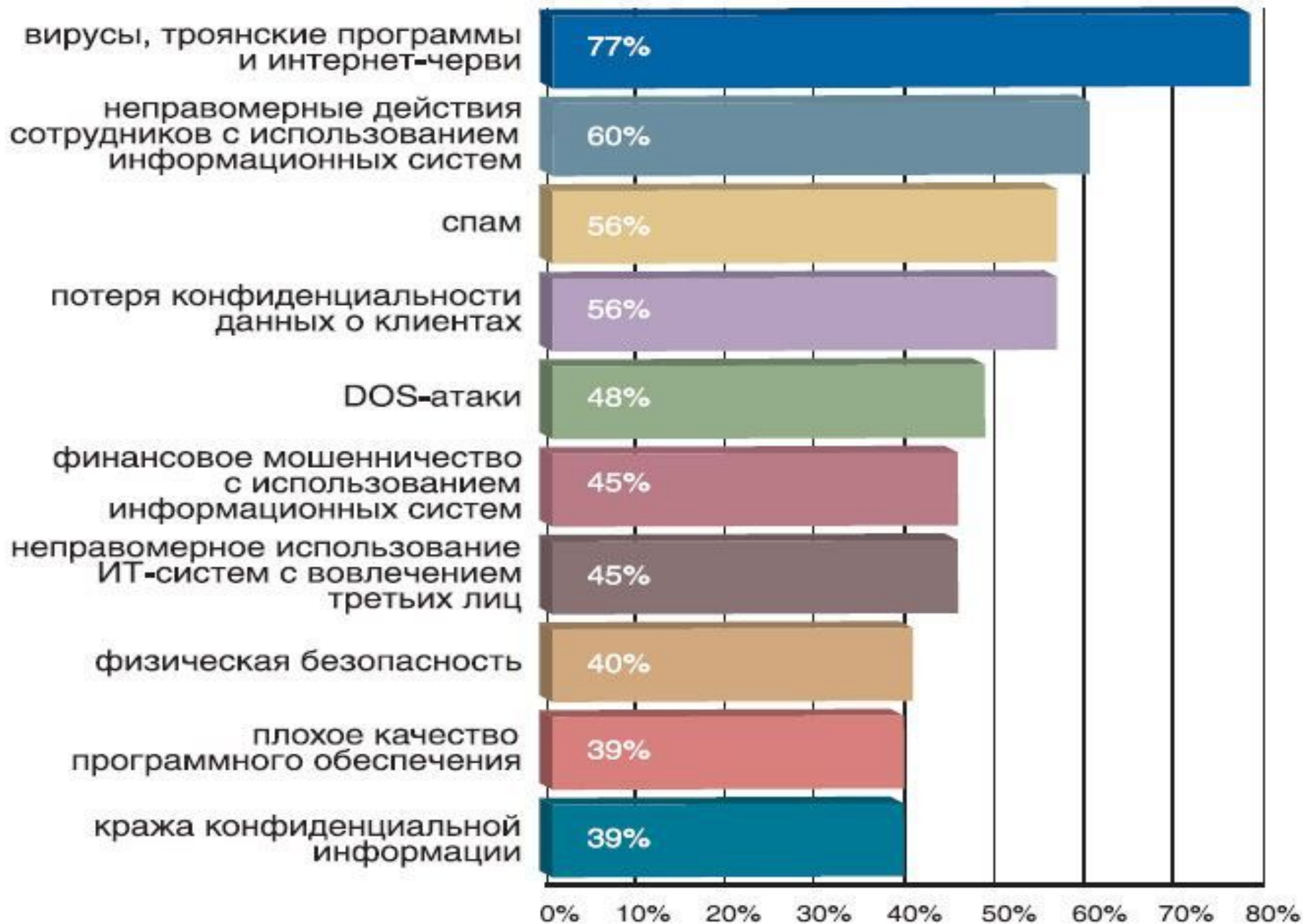
Информационная безопасность
государства

= Защита от информационной агрессии

Информационная безопасность
цивилизации

Защита от всемирных катаклизмов,
потенциально возможных вследствие отказов,
сбоев, ошибок или злоумышленных действий
в ИУС, например, в системах боевого
управления ракетно-ядерным оружием

Десять главных угроз защиты информации



Конфиденциальность

информации — свойство

информации быть доступной только ограниченному кругу конечных пользователей и иных субъектов доступа, прошедших соответствующую проверку и допущенных к ее использованию.




Целостность информации —

свойство сохранять свою структуру и содержание в процессе хранения, использования и передачи.

Достоверность информации — свойство, выражаемое в строгой принадлежности информации субъекту, который является ее источником.





Доступ к информации — возможность субъекта осуществлять определенные действия с информацией.

Санкционированный доступ к информации — доступ с выполнением правил разграничения доступа к информации.

Несанкционированный

доступ (НСД) — доступ

с нарушением правил разграничения


доступа субъекта к информации, с

использованием штатных средств

(программного или аппаратного

обеспечения).





Идентификация — получение от субъекта доступа к сведениям (имя, учетный номер и т.д.), позволяющим выделить его из множества субъектов.

Аутентификация — получение от субъекта сведений (пароль, биометрические параметры и т.д.), подтверждающих, что идентифицируемый субъект является тем, за кого себя выдает.

Угроза информационной безопасности — возможность воздействия на информацию с целью ее искажения, уничтожения, копирования или блокирования, а также возможность воздействия на компоненты компьютерных систем, приводящие к сбою их функционирования.



Уязвимость — любая характеристика, которая может привести к реализации угрозы.

Атака — действия злоумышленника, предпринимаемые с целью обнаружения уязвимости системы защиты и получения несанкционированного доступа к информации.

