



МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ ВЕРОЯТНОСТЕЙ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

КАСАНИН Сергей Николаевич

**заместитель директор по науке государственного
предприятия НИИ ТЗИ, канд. техн. наук, доц.**



ИНФОРМАЦИОННЫЕ СИСТЕМЫ



900 млн долл. в год – продажа устройств подслушивания в США

**8 млрд долл. ежегодно
суммарный урон,
нанесенный организациям,
по отношению к которым
осуществлялось
прослушивание**

**Утечка из организации более
20 % важной внутренней
информации - в 60 случаях
из 100 банкротится**



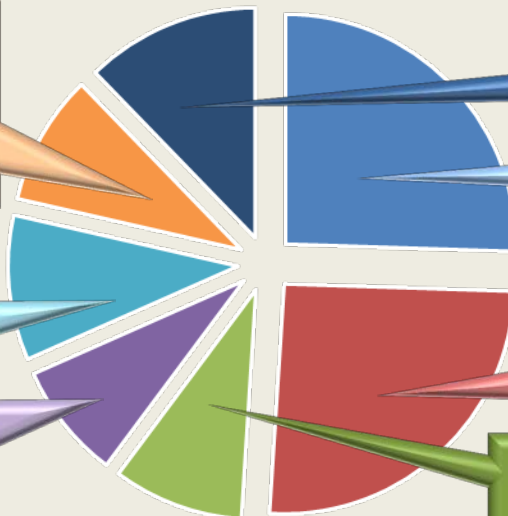
**500 тыс. долл. - средний размер
убытков от одной атаки на
корпоративную систему для
банковского и ИТ-секторов
экономики**

**93 % компаний, лишившихся
доступа к собственной информации
на срок более 10 дней, покинули
бизнес, 50 % заявила о своей
несостоятельности немедленно**

**Срыв работы
информационной системы
– 4-10 %**

**Нарушение доступа
к web-сайтам – 1-11 %**

**Незаконный доступ
сотрудников к информации
– 4-9 %**



**Заражение вредоносными
программами – 11-12 %**

**Кража конфиденциальной
информации – 20-25 %**

**Фальсификация финансовой
информации – 21-25 %**

**Другие виды ущерба
– 14-33 %**

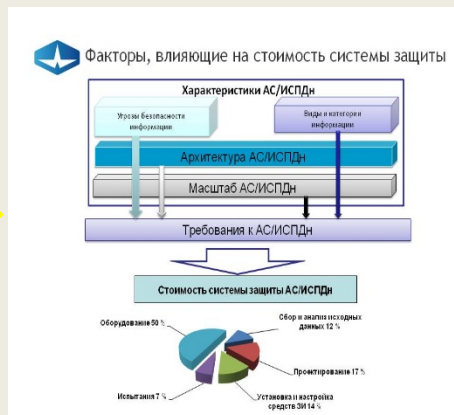


ОПТИМАЛЬНЫЙ УРОВЕНЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

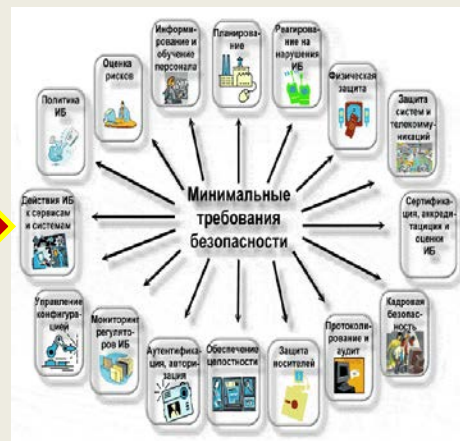


ЗАЩИТА ИНФОРМАЦИИ ДОЛЖНА БЫТЬ
СОРАЗМЕРНОЙ МАСШТАБАМ УГРОЗ!!!

?



?



?



КОРПОРАТИВНЫЕ СЕТИ



**85-97 %
проникновение успешно**

ВОЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ



**88 %
проникновение успешно
390 из 8932 обнаружено
19 сообщено**



ОЦЕНКА ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ





ПОКАЗАТЕЛЬ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ



ВЕРОЯТНОСТЬ ПРЕДОТВРАЩЕНИЯ УГРОЗЫ

ВЕРОЯТНОСТЬ ОБЕСПЕЧЕНИЯ
БЕЗОПАСНОСТИ ИНФОРМАЦИИ

$$P = \prod_{i=1}^I (1 - P_i)$$

1

P_i – вероятность реализации i -й угрозы;

I – общее число возможных угроз

ИНТЕГРАЛЬНЫЙ ПОКАЗАТЕЛЬ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ



СТЕПЕНЬ ЗАЩИЩЕННОСТИ ОИТ ОТ КОМПЛЕКСА УГРОЗ ЗА
ЗАДАННОЕ ВРЕМЯ

$$P = \prod_{i=1}^I (1 - K_i(t) P_i(t))$$

2

$K_i(t)$ – коэффициент опасности угрозы, определяемый в виде четких значений или нечетких множеств для каждой угрозы соответственно



ПОКАЗАТЕЛЬ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ



СРЕДНИЙ РИСК ПРИНЯТИЯ ОПРЕДЕЛЕННЫХ СОСТОЯНИЙ ОБЪЕКТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ВОЗДЕЙСТВИИ УГРОЗ

$$R = \sum_{j=1}^n R_j (x) = \sum_{j=1}^n \sum_{i=1}^I C_{ji} P_{ji} P_i$$

3

P_i – вероятность появления угрозы i -го класса;

P_{ji} – априорная вероятность j -го состояния объекта оценки (ОО) при воздействии угрозы i -го класса;

C_{ji} – потери ОО при принятии им j -го состояния при воздействии угрозы i -го класса;

j – одно из состояний ОИТ, соответствующее одному из возможных событий, которые составляют полную группу несовместимых событий при воздействии угроз



ВЕРОЯТНОСТЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ



СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

**УСТРАНЯЮТСЯ
ВОЗДЕЙСТВИЯ УГРОЗ**

**ОБЕСПЕЧИВАЕТСЯ
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ**

$$P_o = \sum_{j=k} \sum_{i=1}^I P_{ji} P_i$$

4

**При варианте защиты z
 $P_{ji} (P_{ji} = f(z) = P_{jiz})$**

$$P_{oiz} = 1 - P_{iz} = \sum_{j=k} P_{jiz} P_i$$

5

P_{oiz} – вероятность обеспечения безопасности информации от i -й угрозы при z -м варианте защиты информации

7



ВЕРОЯТНОСТЬ РЕАЛИЗАЦИИ i -Й УГРОЗЫ

$$P_{iz} = 1 - \sum_{j=k} P_{jiz} P_i$$

6

ВЕРОЯТНОСТЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ УГРОЗ

$$P_z = \prod_{i=1}^I \left(1 - \sum_{j=k} P_{jiz} P_i \right)$$

7

ОПТИМАЛЬНАЯ СТРАТЕГИИ ПРИНЯТИЯ РЕШЕНИЯ О ВЫБОРЕ ВАРИАНТА ЗАЩИТЫ ИНФОРМАЦИИ, ОБЕСПЕЧИВАЮЩЕЙ МИНИМУМ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ УГРОЗ

$$z = \arg \max_z P_z = \arg \max_z \left\{ \prod_{i=1}^I \left(1 - \sum_{j=k} P_{jiz} P_i \right) \right\}$$

8



ВЕРОЯТНОСТЬ НАРУШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ



СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

НЕУСТРАНЯЮТСЯ
ВОЗДЕЙСТВИЯ УГРОЗ

НЕОБЕСПЕЧИВАЕТСЯ
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

$$P_n = \sum_{j \neq k} \sum_{i=1}^I P_{ji} P_i$$

9

ВЕРОЯТНОСТЬ РЕАЛИЗАЦИИ i -Й УГРОЗЫ ПРИ ВАРИАНТЕ Z

$$P_{iz} = \sum_{j \neq k} P_{jiz} P_i$$

10

9



ВЕРОЯТНОСТЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОТ ВОЗДЕЙСТВИЯ УГРОЗ

$$P_z = \prod_{i=1}^I \left(1 - K_i(t) \sum_{j \neq k} P_{jiz} P_i \right)$$

11

**ОПТИМАЛЬНАЯ СТРАТЕГИЯ ПРИНЯТИЯ РЕШЕНИЯ О ВЫБОРЕ
ВАРИАНТА ЗАЩИТЫ ИНФОРМАЦИИ, ОБЕСПЕЧИВАЮЩЕЙ
МАКСИМУМ СТЕПЕНИ ЗАЩИЩЕННОСТИ (МИНИМУМ
ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ УГРОЗ С УЧЕТОМ
КОЭФФИЦИЕНТА ОПАСНОСТИ УГРОЗ)**

$$z = \arg \max_z P_z = \arg \max_z \left\{ \prod_{i=1}^I \left(1 - K_i(t) \sum_{j \neq k} P_{jiz} P_i \right) \right\}$$

12



Спасибо за внимание!