Технологии и продукты Microsoft в обеспечении ИБ

Лекция 5. Экономика информационной безопасности на примере оценки криптосистем

Цели

- Познакомиться с законодательными и правовыми основами защиты информации
- Рассмотреть основные положения «Закона о персональных данных»
- Изучить принципы разработки политики безопасности
- Проанализировать причины инициативы Microsoft по предоставлению ФСБ и другим заинтересованным государственным организациям доступа к исходному коду своих продуктов

Обоснование затрат на ИБ

- По данным исследований, в западных странах компании тратят на ИБ примерно 5% своего ИТ-бюджета, в России же, по оценкам спецслужб, озвученным на недавнем «Инфофоруме», всего 0,5%. *[2008 г.]*
- «Если бы мы умели разговаривать с финансовыми директорами компаний и объяснять им, почему нужно тратить деньги на ИБ, мы тоже могли бы довести долю расходов на нее до 5%»,

Владимир Мамыкин, директор по информационной безопасности Microsoft в России и СНГ

Из перечня основных направлений и приоритетных проблем научных исследований в области ИБ

46. «Разработка **моделей угроз безопасности систем** и способов их реализации, определение **критериев уязвимости и устойчивости систем** к деструктивным воздействиям…, разработка методологии и методического аппарата оценки ущерба от воздействия угроз информационной безопасности»;

47. «Разработка **методов и средств проведения экспертизы** и контроля качества защиты информации и информационных ресурсов, в том числе вопросов оценки базовых общесистемных программных средств на соответствие требованиям информационной безопасности»;

Методы оценки

- Анализ криптостойкости
- Математическая оценка защищенности информации от несанкционированного доступа, разработанная В.П. Ивановым
- Теория игр
- Методы и инструменты анализа и контроля информационных рисков
- Методы формального анализа криптопротоколов

Методы оценки

- **Анализ криптостойкости**
- Математическая оценка защищенности информации от несанкционированного доступа, разработанная В.П. Ивановым
- Теория игр
- Методы и инструменты анализа и контроля информационных рисков
- Методы формального анализа криптопротоколов

Анализ криптостойкости

- «… it becomes increasingly clear that the term "security" doesn't have meaning unless also you know things like *"Secure from whom?"* or *"Secure for how long?“*»

Методы оценки

- Анализ криптостойкости
  - **Теория игр**
  - Математическая оценка защищенности информации от несанкционированного доступа, разработанная В. П. Ивановым
  - Методы и инструменты анализа и контроля информационных рисков
    - британский CRAMM (Insight Consulting, подразделение Siemens)
    - американский RiskWatch (компания RiskWatch)
    - российский ГРИФ (компания Digital Security).
  - Методы формального анализа криптопротоколов

Теория игр (Bennet S. Yee)

Методы оценки

- Анализ криптостойкости
- ✔ Теория игр
  - **Математическая оценка защищенности информации от несанкционированного доступа, разработанная В.П. Ивановым**
  - Методы и инструменты анализа и контроля информационных рисков
    - британский CRAMM (Insight Consulting, подразделение Siemens)
    - американский RiskWatch (компания RiskWatch)
    - российский ГРИФ (компания Digital Security).
  - Методы формального анализа криптопротоколов

Математическая оценка В.П.Иванова

- Вероятностно-временная группа показателей эффективности защиты:
  - среднее время безопасного функционирования защищаемой системы
  - время безопасного функционирования защищаемой системы с вероятностью ее поражения НСД не выше заданной
  - экономическая эффективность созданной системы защиты информации

Математическая оценка В.П.Иванова

- Аппарат:
  - Решение задачи оценки времени, необходимого злоумышленнику для изучения системы ЗИ **-** с использованием **метрик Холстеда**
  - Среднее время T изучения шифрующей программы злоумышленником:

$$T = 3N^3,$$

где N – длина программы в байтах.

Математическая оценка В.П.Иванова

- Недостатки метода
  - **Границы применимости**: подходит только для оценки *криптосистем ограниченного использования (*по классификации Ж.Брассара), что противоречит *фундаментальному допущению Кирхгоффа*
  - Не учитывает зависимости эффективности криптосистемы от условий ее использования

Методы оценки

- Анализ криптостойкости
- Теория игр
- Математическая оценка защищенности информации от несанкционированного доступа, разработанная В. П. Ивановым
- **Методы и инструменты анализа и контроля информационных рисков**
  - британский CRAMM (Insight Consulting, подразделение Siemens)
  - американский RiskWatch (компания RiskWatch)
  - российский ГРИФ (компания Digital Security).
- Методы формального анализа криптопротоколов

Анализ информационных рисков: CRAMM

- **1:** идентификация и определение ценности защищаемых ресурсов
- **2:** идентификация и оценка угроз в сфере ИБ, поиск и оценка уязвимостей защищаемой системы
- **3:** генерация вариантов мер противодействия выявленным рискам:
  - рекомендации общего характера;
  - конкретные рекомендации;
  - примеры того, как можно организовать защиту в данной ситуации.
- **Недостатки** метода:
  - не учитывает специфики СКЗИ!

Методы оценки

- Анализ криптостойкости
- Теория игр
- Математическая оценка защищенности информации от несанкционированного доступа, разработанная В.П. Ивановым
- Методы и инструменты анализа и контроля информационных рисков
- **Методы формального анализа криптопротоколов**

Методы формального анализа криптопротоколов

- **Классы методов**:
  - Дедуктивные методы
  - Методы анализа состояний
  - Методы статического анализа

- **Недостатки**:
  - Абстрагируются от деталей реализации в предположении, что используемые методы шифрования идеальны

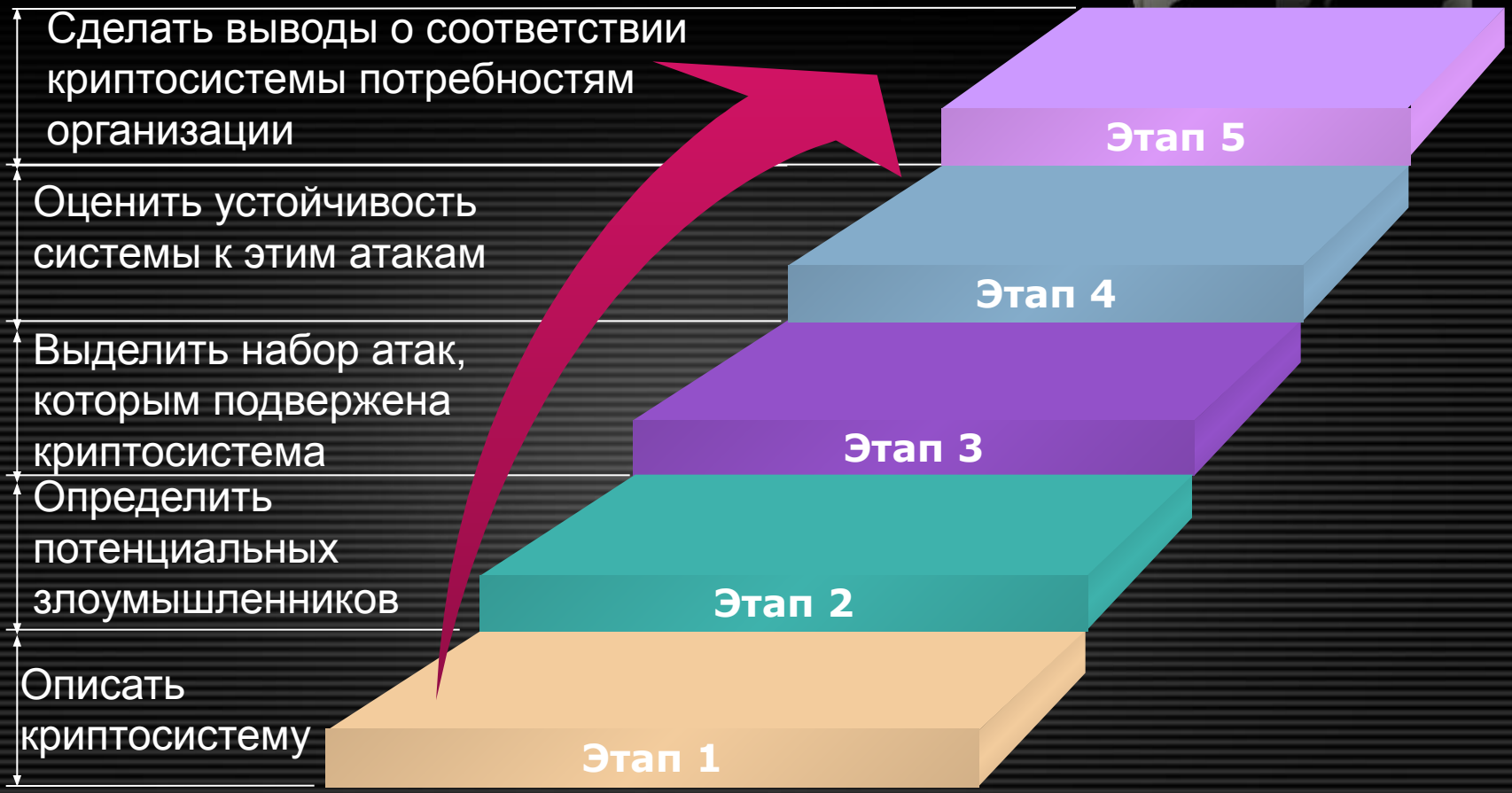
Сравнительный анализ

Метод оценки	Применимость	Экономические показатели	Возможности злоумышленника
Анализ криптостойкости	+	-	±
Теория игр / Мат. модель В.П.Иванова	±	+	-
Анализ информационных рисков	-	+	+
Анализ криптопротоколов	±	-	-

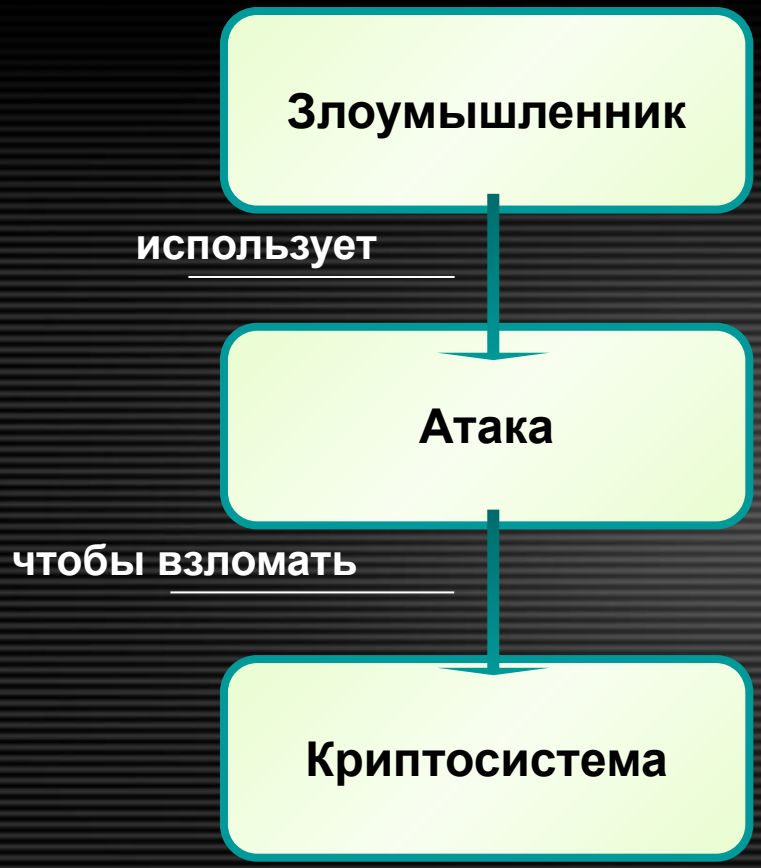
Цели и задачи

- Разработка формальной модели оценки эффективности криптосистемы в заданном контексте использования
- Разработка инструментальных средств для оценки стойкости криптосистем к различным видам атак
- Систематизация и анализ методик оценки экономической эффективности инвестиций в обеспечение информационной безопасности

Процесс оценки эффективности криптосистемы

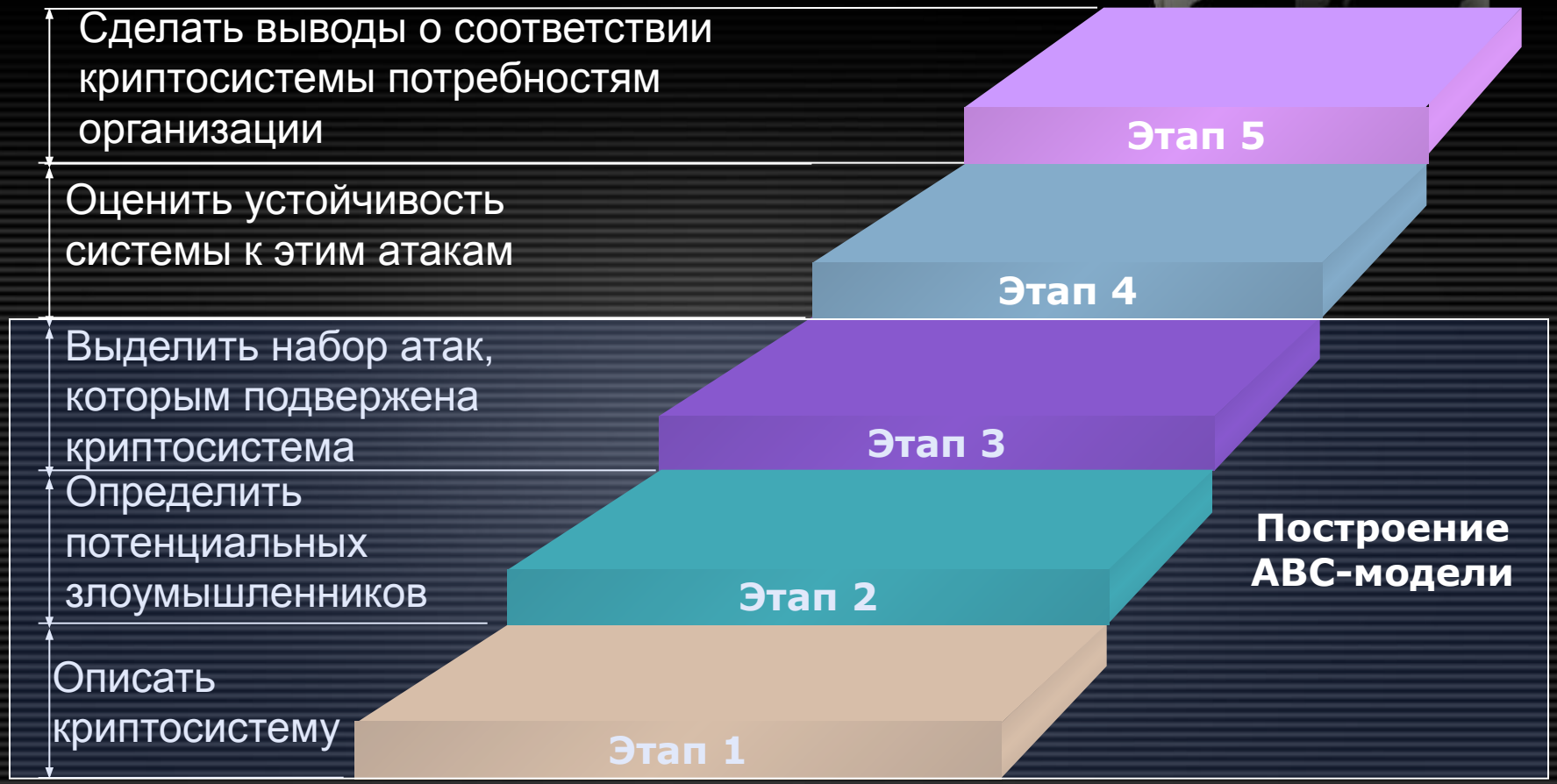


ABC-модель угроз



- “A” от *Attack*
- “B” от *code-Breaker*
- “C” от *Cryptosystem*

Процесс оценки эффективности криптосистемы



Классификация криптосистем

- Классификация **Ули Маурера** (Ueli Maurer) - по количеству ключей
  - Бесключевые
  - Одноключевые
  - Двухключевые

- Классификация **Жиля Брассара** (Gilles Brassard) - по секретности алгоритма шифрования
  - Криптосистемы ограниченного использования
  - Криптосистемы общего использования

Классификация криптосистем

- **По доступности информации о криптоалгоритме**
  - Криптосистемы ограниченного использования
  - Криптосистемы общего использования
- **По количеству ключей**
  - Бесключевые
  - Одноключевые
  - Двухключевые
  - Многоключевые
- **По стойкости криптоалгоритма**
  - Безусловно стойкие
  - Доказуемо стойкие
  - Предположительно стойкие
- **По используемым средствам шифрования**
  - Программные
  - Аппаратные
  - Программно-аппаратные
- **По наличию сертификата**
  - Сертифицированные
  - Несертифицированные

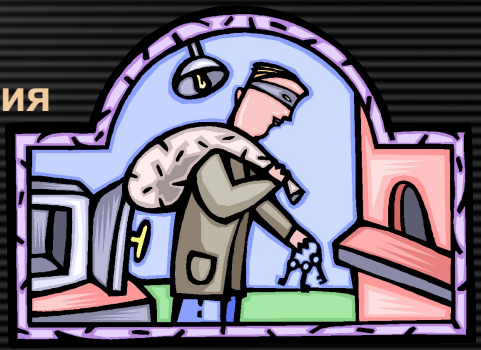
Классификация взломщиков

- **Модель нарушителя должна учитывать:**
  - Категории лиц, в числе которых может оказаться нарушитель;
  - Предположения о квалификации нарушителя и его технической оснащённости;
  - Возможные цели нарушителя и ожидаемый характер его действий.

- **Классификация Брюса Шнайера – по движущим мотивам:**
  - Взломщики, в основе мотивации которых лежит корыстный интерес;
  - Взломщики, в основе мотивации которых лежат эмоциональные побуждения;
  - Друзья/родственники;
  - Промышленные конкуренты;
  - Пресса;
  - Правительство;
  - Полиция;
  - Научно-исследовательские организации.

Классификация взломщиков

- **по технической оснащенности**
  - Персональный компьютер
  - Сеть ЭВМ
  - Суперкомпьютер
- **по конечной цели**
  - Обнаружение слабости в алгоритме
  - Полный взлом алгоритма
- **по доступу к шифрующим средствам**
  - «внутренний» нарушитель
  - «внешний» нарушитель
- **по уровню подготовки**
  - Взаимодействие с компьютером на уровне пользователя
  - Математический аппарат
  - Программирование
  - Электротехника и физика
  - Социальная инженерия
- **по первичной информации о средстве шифрования**
  - пользователь
  - криптограф
  - «клептограф»
- **по возможности кооперации**
  - «Одиночка»
  - Коллектив



Классификация атак

- Классическая **классификация Кирхгоффа** по доступу к открытому и зашифрованному тексту с появлением **атак по побочным каналам** уже не может считаться полной.

- Современные схемы для описания атак на компьютерные системы
  - **Landwehr C.E., Bull A.R.** A taxonomy of computer program security flaws, with examples // ACM Computing Surveys, 26(3): p. 211–254, September 1994.
  - **Lindqvist U., Jonsson E.** How to systematically classify computer security intrusions. // IEEE Symposium on Security and Privacy, p. 154–163, Los Alamitos, CA, 1997.
  - **Paulauskas N., Garsva E.** Computer System Attack Classification // Electronics and Electrical Engineering 2006. nr. 2(66)
  - **Weber D. J.** A taxonomy of computer intrusions. Master's thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, June 1998.

Классификация атак

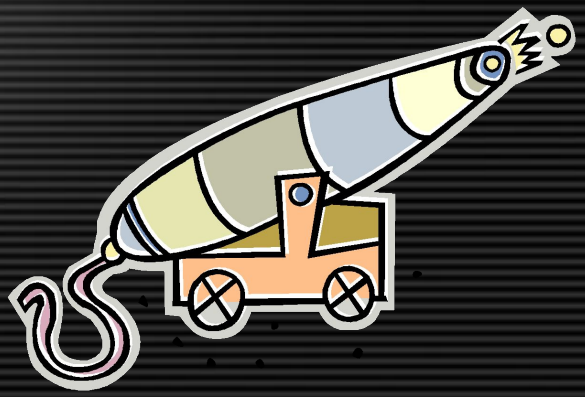
- Классическая **классификация Кирхгоффа** по доступу к открытому и зашифрованному тексту с появлением **атак по побочным каналам** уже не может считаться полной.

- Современные схемы для описания атак на компьютерные системы
  - **Landwehr C.E., Bull A.R.** A taxonomy of computer program security flaws, with examples // ACM Computing Surveys, 26(3): p. 211–254, September 1994.
  - **Lindqvist U., Jonsson E.** How to systematically classify computer security intrusions. // IEEE Symposium on Security and Privacy, p. 154–163, Los Alamitos, CA, 1997.
  - **Paulauskas N., Garsva E.** Computer System Attack Classification // Electronics and Electrical Engineering 2006. nr. 2(66)
  - **Weber D. J.** A taxonomy of computer intrusions. Master's thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, June 1998.

Не подходят для идентификации криптоатак!

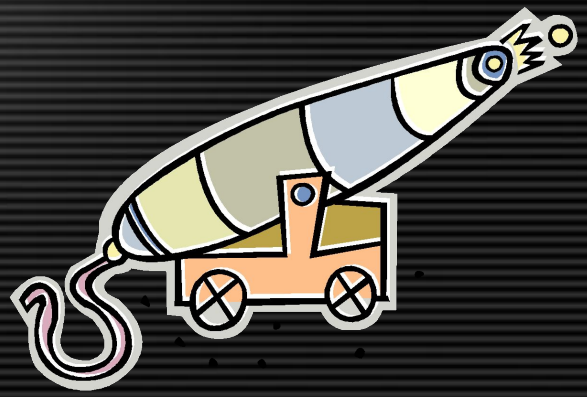
Классификация атак (1/2)

- **по доступу к открытому и зашифрованному тексту на основе:**
  - только шифртекста
  - открытого текста
  - подобранного открытого текста
  - адаптивно подобранного открытого текста
  - информации из побочных каналов
- **по контролю над процессом**
  - пассивные
  - активные
- **по исходу атаки**
  - полный взлом
  - глобальная дедукция
  - частичная дедукция
  - информационная дедукция
- **по критическим ресурсам**
  - память
  - время
  - данные



Классификация атак (2/2)

- **по степени применимости к различным шифрам**
  - универсальные
  - для определенной категории шифров
  - для конкретного криптоалгоритма
- **по используемым средствам**
  - математические методы
  - устройства перехватчики физических параметров процесса шифрования
  - эволюционное программирование
  - квантовые компьютеры
- **по последствиям**
  - нарушение конфиденциальности
  - нарушение целостности
  - нарушение доступности
- **по возможности распараллеливания**
  - распределенные
  - не распределенные



Классификации

- **Классификация криптосистем**
  - по доступности информации о криптоалгоритме
  - по количеству ключей
  - по стойкости криптоалгоритма
  - по используемым средствам шифрования
  - по наличию сертификата

- **Классификация взломщиков**
  - по технической оснащенности
  - по конечной цели
  - по доступу к шифрующим средствам
  - по уровню подготовки
  - по первичной информации о средстве шифрования
  - по возможности кооперации

- **Классификация атак**
  - по доступу к открытому и зашифрованному тексту
  - по контролю над процессом
  - по исходу атаки
  - по критическим ресурсам
  - по степени применимости к различным шифрам
  - по используемым средствам
  - по последствиям
  - по возможности распараллеливания

Модель угроз как композиция модели криптосистемы, злоумышленника и атаки

Параметрическая модель **атаки**: $a \in A$
где $A = A_1 \times A_2 \times \ldots \times A_8$, $A_j (j = \overline{1, 8})$ - множество значений j-го параметра модели атаки

Параметрическая модель **злоумышленника**: $b \in B$
где $B = B_1 \times B_2 \times \ldots \times B_6$, $B_j (j = \overline{1, 6})$ - множество значений j-го параметра модели злоумышленника

Параметрическая модель **криптосистемы**: $c \in C$
где $\Sigma = C_1 \times C_2 \times \ldots \times C_5$, $C_j (j = \overline{1, 5})$ - множество значений j-го параметра модели криптосистемы

Математическая модель оценки эффективности криптосистемы

Риск

$$\hat{A}(\vec{a},\vec{b},\vec{c}) = I(\vec{a},\vec{c}) \times R(\vec{a},\vec{b})$$

Влияние

$$I : A' \pounds \to [0;1]$$

$$I(\vec{a},\vec{c}) = \min_{h=\overline{1,8}} \tilde{O}_{g=\overline{1,5}} \overline{I_{gh}}(c_g, a_h)$$

$$\overline{I_{gh}} : C_g' A_h \to [0;1],\ g = \overline{1,5},\ h = \overline{1,8}$$

$$\overline{I_{gh}}(c,a) = \frac{I_{gh}(c,a)}{\sum_{x \in C_g} I_{gh}(x,a)}$$

$$I_{gh} : C_g' A_h \to i_+$$

Вероятность

$$R : A' B \to [0;1]$$

$$R(\vec{a},\vec{b}) = \min_{h=\overline{1,8}} \tilde{O}_{t=\overline{1,6}} \overline{R_{th}}(b_t, a_h)$$

$$\overline{R_{th}} : B_t' A_h \to [0;1],\ t = \overline{1,6},\ h = \overline{1,8}$$

$$\overline{R_{th}}(b,a) = \frac{R_{th}(b,a)}{\sum_{b \in B_t} R_{th}(b,a)}$$

$$R_{th} : B_t' A_h \to i_+$$

Критерий эффективности

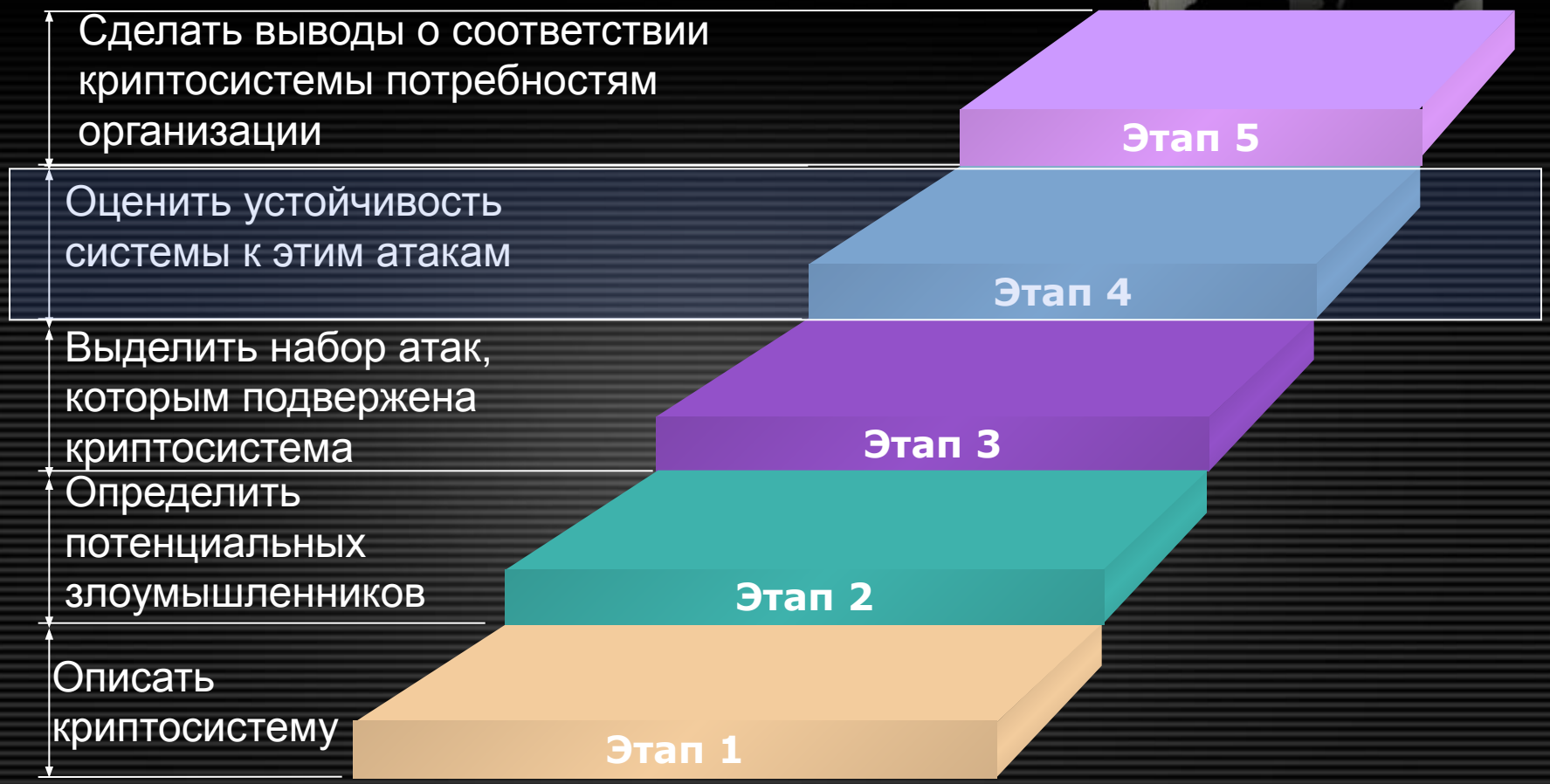
За критерий эффективности **криптосистемы**, состоящей из подсистем $\vec{c} \in £ ¢(£ ¢' £)$, в условиях, когда ей угрожают **злоумышленники** $\vec{b} \in B ¢(B ¢' B)$, примем ее способность противостоять **атакам**, входящим в множество

$$L = \bigcup_{\vec{b} \in B ¢} \bigcup_{\vec{c} \in C ¢} I(\vec{b}, \vec{c}),$$

где $I(\vec{b}, \vec{c}) = \{ \vec{a} \in A : \hat{A}(\vec{a}, \vec{b}, \vec{c}) > q \}$,

$q \in [0; 1]$ - заданное пороговое значение риска

Процесс оценки эффективности криптосистемы



Оценка устойчивости

- Опубликованная статистика
  - *www.distributed.net:* вскрытие RC5-64 методом «распределенного взлома»
    - более 300 тысяч пользователей глобальной сети,
    - время перебора: пять лет (1757 дней)
    - 85% всего пространства ключей
- А что, если:
  - опубликованной статистики нет,
  - шифр новый,
  - математические открытия привели к возможности ранее не использовавшегося типа атаки?

Доступные средства для криптоанализа

- Библиотеки функций для работы с длинной арифметикой
- Математические пакеты **Maple** и **Mathematica**

Решение / Критерии оценки	Mathematica	LIP	CLN	LiDIA	GMP	NTL
Эффективность вычислений						
Возможность сборки в ОС Windows						
Наличие алгоритмов работы с разреженными матрицами						
Наличие алгоритмов создания факторной базы, решета и разложения на множители						
Удобство пользовательского интерфейса						

Доступные решения

- Математические пакеты **Maple** и **Mathematica**
  - «+»: простота кодирования алгоритмов
  - «+»: нет ограничений на разрядность
  - «-»: платформенная зависимость
  - «-»: низкая эффективность

Доступные решения (2/3)

- Встроенные числовые типы языков **C** и **C++** имеют ограниченную разрядность
  - `long` – 32 бита
  - `long long` – 64 бита
  - `double`: 53 бита – мантисса, 11 бит – экспонента
  - `long double`: 64 бита – мантисса, 15 бит - экспонента
- **Java** поддерживает возможность работы с длинными числами
  - «+»: переносимость
  - «-»: низкая эффективность

Доступные решения

- **Библиотеки функций для работы с длинной арифметикой**
  - «+»: высокая эффективность
  - «+»: большой выбор решений в открытом доступе *(LIP, LiDIA, CLN, PARI, GMP, MpNT)*

LIP (Large Integer Package)

- Библиотека для работы с длинной арифметикой
- Авторы: Arjen K. Lenstra, Paul Leyland
- Одна из первых библиотек
- Язык: ANSI C
- «+»: переносимость
- «-»: низкая эффективность

CLN (a Class Library for Numbers)

- Реализует элементарные арифметические и логические функции
- Авторы: Bruno Haible, Richard Kreckel
- Язык: C++
- Большой набор классов:
  - Целые числа
  - Рациональные числа
  - Числа с плавающей запятой
  - Комплексные числа
  - Модулярная арифметика
- «-» универсальная числовая библиотека => ограниченная применимость для решения узкоспециализированных задач.

LiDIA

- Автор: Thomas Papanikolau (Technical University of Darmstadt)
- Язык: C++
- Поддерживает различные пакеты для работы с целыми числами *(Berkley MP, GMP, CLN, libI, LIP)*
- Высокоэффективные реализации:
  - типов данных с увеличенной точностью
  - алгоритмов с большой временной сложностью
- «-»: невозможность сборки в операционных системах Windows

GMP (GNU Multiple Precision arithmetic library)

- Библиотека теоретико-числовых алгоритмов
- Автор: Torbjord Granlund (free software group)
- Язык: C, ASM
- Упор на скорость
- Эффективность растет при увеличении разрядности операндов
- «-»: невозможность сборки в операционных системах Windows
- «-»: отсутствие алгоритмов формирования факторной базы, решета, разложения на множители

NTL (a Library for doing Number Theory)

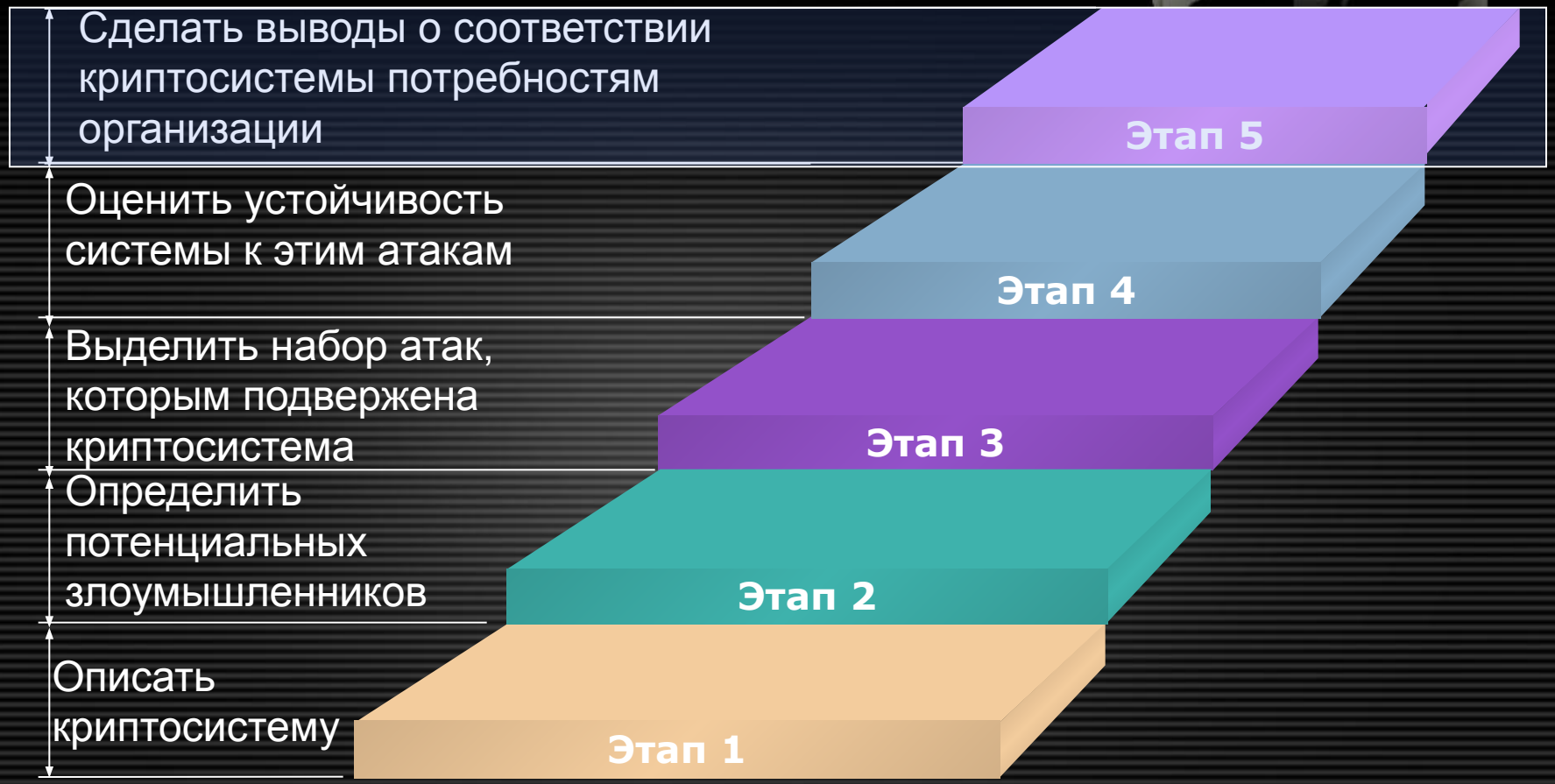
- Библиотека теоретико-числовых алгоритмов
- Автор: Victor Shoup
- Язык: C++
- Переносимость
- Высокоэффективные реализации:
  - полиномиальной арифметики
  - решеток
- Для повышения эффективности можно использовать совместно с GMP
- «-»: отсутствие алгоритмов формирования факторной базы, решета, разложения на множители

Доступные средства для криптоанализа

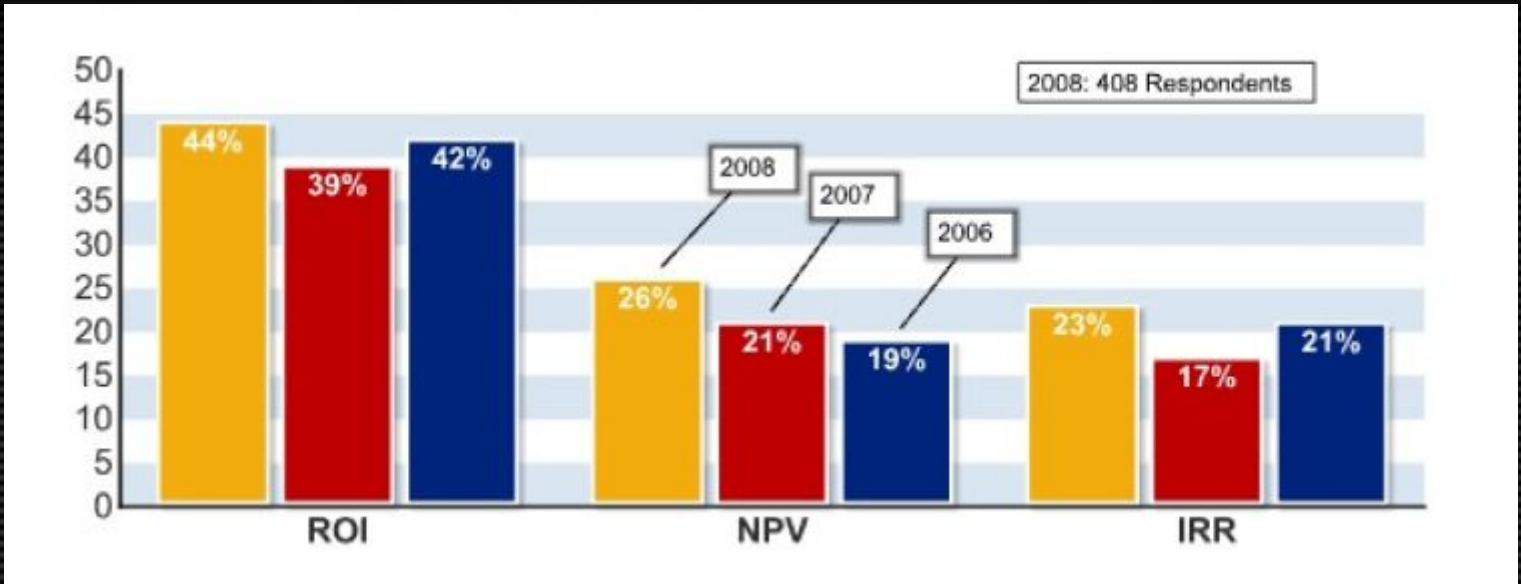
- Библиотеки функций для работы с длинной арифметикой
- Математические пакеты **Maple** и **Mathematica**

Решение / Критерии оценки	Mathematica	LIP	CLN	LiDIA	GMP	NTL
Эффективность вычислений	-	-	-	-	+	+
Возможность сборки в ОС Windows	+	+	+	-	-	+
Наличие алгоритмов работы с разреженными матрицами	-	-	-	+	+	-
Наличие алгоритмов создания факторной базы, решета и разложения на множители	-	-	-	+	-	-
Удобство пользовательского интерфейса	+	-	-	-	-	-

Процесс оценки эффективности криптосистемы



Использование метрик ROI, NPV, IRR*



* Источник: CSI Computer Crime & Security Survey 2008, http://www.gocsi.com/

Выбор методики оценки экономической эффективности

Методика оценки	Преимущества	Недостатки
Коэффициент возврата инвестиций (ROI)	▪ Показатель, понятный финансистам	▪ Отсутствие достоверных методов расчета ▪ «Статичный» показатель
Совокупная стоимость владения (TCO)	▪ Позволяет оценить целесообразность реализации проекта на основании только затрат ▪ Предполагает оценку затрат на различных этапах ЖЦ системы	▪ Не учитывает качество системы безопасности ▪ «Статичный» показатель ▪ Показатель, специфичный для ИТ
Дисконтированные показатели эффективности инвестиций	▪ Показатель, понятный финансистам ▪ Учитывает зависимость потока денежных средств от времени ▪ Учитывает все потоки денежный средств, связанные с реализацией проекта	▪ Сложность расчета

Метод дисконтированных показателей

- Для определения эффективности инвестиционного проекта оцениваются:
  - Чистый дисконтированный доход (NPV),
  - Внутренняя норма доходности (IRR),
  - Индекс доходности (PI),
  - Срок окупаемости с учетом дисконтирования ($T_{ок}$)

Расчет эффективности инвестиций

- Стоимость внедрения СКЗИ: 120 000,00 р.
- Ценность защищаемой информации: 205 000,00 р./г.
- Сокращение риска НСД: 1 год - 95%, 2 год – 70%, 3 год – 35%
- Финансовые потоки (ставка дисконтирования: 20,8%):

Периоды	0	1	2	3
Первоначальные инвестиции	- 120 000, 00			
Выгоды (мат. ожидание прибыли от использования информации)		194 750, 00	153 750, 00	61 500, 00
Стоимость годовой поддержки		-55 000, 00	-55 000, 00	-55 000, 00
Затраты на администрирование		-30 000, 00	-30 000, 00	-30 000, 00
Итого:	- 120 000, 00	109 750, 00	68 750, 00	- 23 500, 00

- NPV = 4 574,20 р.
- IRR = 26,5%
- PI =1.04 (PI < 1,2%)

Выводы

«As information security is about power and money …, the evaluator should not restrict herself to technical tools like cryptanalysis and information flow, but also apply economic tools»

Ross Anderson,
Professor in Security Engineering at the University of Cambridge Computer Laboratory

Использованные источники

- **Мамыкин В.** Тенденции рынка информационной безопасности // IT-Summit'2008, Опубликовано: http://blogs.technet.com/mamykin/attachment/3035627.ashx
- **Авдошин С.М., Савельева А.А.** О новом подходе к проблеме анализа эффективности криптосистем // Информационные технологии. 2009. № 8. С. 2-9.


Спасибо за внимание!
Вопросы?