Efficiency Evaluation of Cryptographic Protection of Information in Enterprise Applications

Sergey Avdoshin
Head of Software Engineering Department, State University – Higher School of Economics, Russia
email: savdoshin@hse.ru

Alexandra Savelieva
Lecturer, State University – Higher School of Economics, Russia
email: asavelieva@hse.ru

Abstract

We introduce a complex approach to evaluating cryptographic protection efficiency. Classically, the research has mostly focused on information system security as a whole, whereas cryptographic tools evaluation techniques have not received as much attention. The main thread of our work is the development of mathematical models of threats to analyze the security of cryptographic systems based on various types of attacks that the cryptographic system is exposed to. The approach allows to build an economic rationale for investments to cryptographic systems and to provide sound arguments for implementing an information security strategy.

***Keywords**: cryptographic system, cryptanalysis, threat modeling.*

Оценка эффективности криптографической защиты информационных ресурсов в корпоративных системах

Сергей Авдошин
Государственный университет – Высшая школа экономики
Руководитель отделения программной инженерии
email: savdoshin@hse.ru

Александра Савельева
Государственный университет – Высшая школа экономики
Преподаватель
email: asavelieva@hse.ru

Краткая аннотация

В данной статье предлагается комплексный подход к оценке эффективности защиты информационных ресурсов предприятия, обеспечиваемой криптографическими средствами. Разработанная методика позволяет провести экономическое обоснование расходов организации на обеспечение информационной безопасности и сделать обоснованный выбор мер и средств криптографической защиты. В основе методики лежит формализованный процесс анализа надежности криптосистемы в определенном контексте использования и математическая модель угроз безопасности защищаемых информационных ресурсов.

***Ключевые слова**: СКЗИ, криптоанализ, моделирование угроз.*

1. Введение

Средства криптографической защиты информации (СКЗИ) представляют собой средства вычислительной техники, осуществляющие криптографическое преобразование информации для обеспечения ее конфиденциальности и контроля целостности [1].

При оценке эффективности СКЗИ важнейшим критерием считается криптостойкость. Такой подход не учитывает других важных требований к криптосистемам. Обоснованный выбор методов криптографической защиты информации для конкретных информационных систем должен опираться не только на криптостойкость, но и на

другие критерии эффективности, такие как (см. [2]):

- минимальный объем используемой ключевой информации;
- минимальная сложность реализации (в количестве машинных операций);
- стоимость;
- высокое быстродействие.

Анализ публикаций в открытом доступе показал, что подходящие методики оценки эффективности криптографических систем до сих пор не разработаны (к аналогичным выводам пришли авторы работы [2]). Исключением является статья В.П.Иванова [3], в которой эффективность криптографических средств защиты предлагается оценивать с использованием математического аппарата теории массового обслуживания и теории катастроф на основе *вероятностно-временной группы показателей*, в числе которых:

- среднее время безопасного функционирования защищаемой системы;
- время безопасного функционирования защищаемой системы с вероятностью НСД не выше заданной;
- экономическая эффективность созданной системы защиты информации.

Выбор показателей эффективности представляет интерес, однако методика имеет ряд критических недостатков, которые делают невозможным ее применение на практике для оценки современных СКЗИ. В первую очередь это границы применимости: методика подходит только для оценки криптосистем, принадлежащих по классификации Ж.Брассара [4] к классу *криптосистем ограниченного использования*, стойкость которых основывается на сохранении в секрете алгоритмов зашифрования и расшифрования. Однако, согласно фундаментальному допущению Кирхгоффа [5], стойкость криптосистемы должна основываться не на секретности алгоритмов зашифрования и расшифрования, а на секретности некоторого значения, которое называется ее *ключом*. Все современные криптосистемы построены по этому принципу, и исследования их надежности всегда должны проводиться в предположении, что потенциальному противнику о криптосистеме известно все, за исключением используемого ключа.

Еще одним недостатком описанной в работе [3] методики является то, что она не учитывает зависимости эффективности криптосистемы от условий ее использования. Очевидно, эффективность одной и той же криптосистемы в разных контекстах может существенно отличаться. Среда функционирования системы накладывает определенные ограничения на возможные сценарии атак. Простая модель сценария атаки представлена на рис. 1 [6]. Она включает три элемента, каждый из которых оказывает влияние на общую картину угроз. Типы атак, которым подвержена криптосистема, зависят от навыков, уровня доступа, бюджета и других характеристик потенциальных злоумышленников [7]. Информация, подлежащая защите, определяет возможных злоумышленников, которые могут осуществлять попытки взлома в целях нарушения конфиденциальности, целостности или доступности (во избежание избыточности из модели исключен элемент «Защищаемые ресурсы», который задается неявно - через элемент «Злоумышленник»).

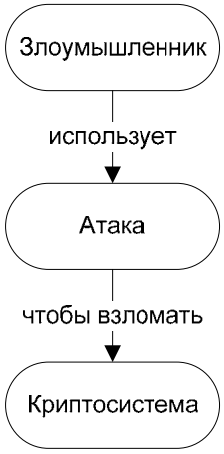

Рисунок 1 - Сценарий взлома криптосистемы

Использование СКЗИ, обеспечивающих устойчивость к взлому ниже некоторой «фоновой» вероятности, является экономически неоправданным [8]. Например, если вероятность выхода компании из бизнеса равна 2^{-30} (менее чем один из миллиона), то есть ли смысл для защиты информации, которая может нанести компании ущерб, сопоставимый с кризисом рынка, использовать алгоритм, вероятность вскрытия которого за приемлемое время составляет 2^{-200}?

Наиболее эффективным при выборе и оценке криптографической системы считается использование экспертных оценок и имитационное моделирование [2]. Разработаны методы и средства, позволяющие построить модели угроз и уязвимостей информационных систем и на основе анализа рисков получить количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. В работах Н.Кукановой [9, 10] описаны методы и инструменты анализа и контроля

информационных рисков: британский CRAMM [11] (компания Insight Consulting, подразделение Siemens), американский RiskWatch [12] (компания RiskWatch) и российский ГРИФ [13] (компания Digital Security). Эти инструментальные средства полезны специалисту при проведении аудита систем обеспечения безопасности предприятия, однако они не учитывают специфики СКЗИ.

Для оценки эффективности СКЗИ необходимы методики, позволяющие принимать во внимание взаимосвязь типов криптосистемы, потенциальных злоумышленников и возможных атак на защищаемые информационные ресурсы.

2. Постановка задачи

Задача состоит в разработке методики анализа эффективности криптографической системы с учетом того, каким угрозам защищаемая информация будет подвергаться со стороны злоумышленников.

В качестве исходных данных для проведения оценки эффективности криптографической защиты информационных ресурсов используются данные об особенностях реализации исследуемой криптосистемы и типах потенциальных злоумышленников. Анализ эффективности осуществляется на основе финансово-экономических показателей СКЗИ. Оценка эффективности создает предпосылку для определения соответствия криптосистемы потребностям организации, принятия решений и осуществления мер по отказу от СКЗИ, не обеспечивающих необходимый уровень защиты, и внедрению систем, достигших наилучших значений показателей.

Для решения поставленной задачи необходимо:

- Формализовать процесс оценки эффективности криптографической защиты;
- Разработать математическую модель угроз безопасности информационных ресурсов, защищенных с использованием криптографических средств.
- Провести анализ существующих методов оценки СКЗИ с экономических позиций.
- Выбрать финансово-экономические показатели, подходящие для экономической оценки инвестиций в СКЗИ.

3. Процесс оценки эффективности криптографической защиты

Процесс оценки эффективности криптографической защиты можно представить в виде схемы на рис.2 [6].

Цель каждого этапа – получение ответа на вопрос:

- Этап 1: Какая криптосистема является объектом атаки?
- Этап 2: Кто будет атаковать эту криптосистему?
- Этап 3: Какие методы криптоанализа с наибольшей вероятностью будут использованы при осуществлении попыток взлома криптосистемы?
- Этап 4: Способна ли криптосистема противостоять таким атакам?
- Этап 5: Является ли использование исследуемой криптосистемы экономически выгодным в данном контексте?

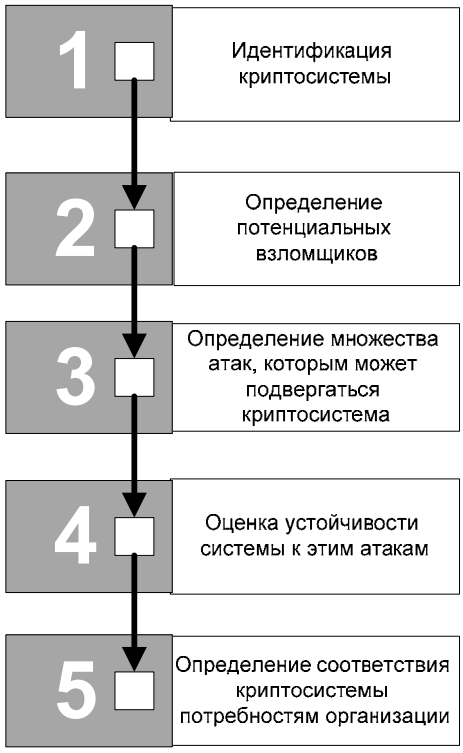

Рисунок 2 - Процесс оценки эффективности криптографической защиты

Этапы 1-3 направлены на моделирование угроз, которым подвергаются информационные ресурсы, защищаемые с использованием исследуемой криптосистемы. Первый этап - определение объекта исследования. Здесь описываются конкретные характеристики криптосистемы. На втором этапе задаются параметры, определяющие тип потенциальных взломщиков криптосистемы. Между

характеристиками криптосистемы и возможными типами атак существует связь. Аналогично, навыки, уровень доступа, бюджет в распоряжении злоумышленника определяют типы атак, которые он может предпринять [7]. Таким образом, при наличии формальных представлений исследуемой криптосистемы и потенциальных злоумышленников мы можем перейти к этапу 3 на рис.2, т.е. определить типы атак, которым подвержена криптосистема, а также вероятность их реализации.

Этап 4 представляет собой анализ устойчивости криптосистемы к атакам, определенным на этапе 3. Необходимо обеспечить специалиста набором инструментальных средств для проведения исследований. Программный комплекс [14, 15], описанный в [6], предназначен для оценки стойкости асимметричных криптосистем к современным методам криптоанализа. Цель этапа 4 – оценить риск нарушения безопасности информационных ресурсов, защищенных с использованием исследуемой криптосистемы.

Наконец, этап 5 предполагает использование различных подходов к оценке экономической эффективности инвестиций в СКЗИ на основании данных, полученных на этапах 1-4.

4. Математическая модель угроз безопасности информационных ресурсов

Задача оценки криптографической защищенности информационных ресурсов сводится к выделению подмножества атак, которым может подвергаться криптосистема в данном контексте использования, и определению устойчивости системы к этим атакам. Под устойчивостью системы будем понимать ее *криптостойкость*, т.е. способность противостоять атакам криптоаналитика [16].

Определение криптостойкости является научной задачей, для решения которой необходим набор инструментальных средств, позволяющих моделировать поведение злоумышленника при попытках взлома системы с использованием различных методов криптоанализа (см., например, [17]). Описание реализации программного комплекса, предназначенного для исследования стойкости асимметричных криптосистем с использованием математических методов, выходит за рамки данной статьи и приведено в [6].

Для определения эффективности криптосистемы имеет смыл проверять ее устойчивость не ко всем возможным атакам, а к тем, которые представляют для нее наибольшую угрозу. Состав множества потенциально опасных атак зависит от типа криптосистемы и условий использования криптосистемы.

Для выделения набора атак, которым подвержена криптосистема, построим математическую модель угроз безопасности защищаемых информационных ресурсов, основываясь на следующих предпосылках:

- Один взломщик может предпринять атаки различного типа, а одна и та же атака может исходить от разных взломщиков;
- К одной и той же криптосистеме применимы атаки различного типа, а одна и та же атака позволяет взломать различные криптосистемы;
- Злоумышленник с наибольшей вероятностью выберет ту атаку, которая обеспечит максимальный результат при фиксированных затратах, либо наименее затратный вариант из множества атак, приводящих к одинаковому результату.

Пусть $\mathrm{A} \subseteq A_1 \times A_2 \times ... \times A_8$ - множество параметрических моделей атак, где A_j ($j = \overline{1, 8}$) - множество значений $j-$го параметра модели атаки, определяющего тип атаки в соответствии с критериями разработанной классификации (см. [18]):

A_1 - по доступу к открытому коду;

A_2 - по контролю над процессом шифрования;

A_3 - по исходу атаки;

A_4 - по объему необходимых ресурсов;

A_5 - по степени применимости к различным шифрам;

A_6 - по используемым средствам;

A_7 - по последствиям атаки;

A_8 - по возможности распараллеливания.

Каждая модель $\vec{a} \in \mathrm{A}$ представляет собой вектор $\left(a_1, a_2, \ ... \ , a_8\right)$, где $a_j \in A_j$, $j = \overline{1, 8}$. Заметим, что, поскольку множества значений параметров модели атаки конечны, то мощность множества моделей атак $\mid \mathrm{A} \mid \leq \prod_{j=1}^{8} \mid A_j \mid$.

Пусть $\mathrm{B} \subseteq B_1 \times B_2 \times ... \times B_6$ - множество параметрических моделей злоумышленников, где B_j ($j = \overline{1, 6}$) - множество значений $j-$го параметра модели злоумышленника в соответствии с критериями описанной в [18] классификации:

B_1 - по технической оснащенности;

B_2 - по конечной цели;

B_3 - по доступу к шифрующим средствам;

B_4 - по уровню подготовки;

B_5 - по первичной информации о средстве шифрования;

B_6 - по возможности кооперации.

Каждая модель $\vec{b} \in \mathrm{B}$ задана в виде вектора $\left(b_1, b_2, \ \dots \ , b_6\right)$, где $b_j \in B_j$, $j = \overline{1,\,6}$, $|\ \mathrm{B}\ | \leq \prod_{j=1}^{6} |\ B_j\ |$.

Пусть $\mathrm{C} \subseteq C_1 \times C_2 \times \ldots \times C_5$ - множество параметрических моделей криптосистем, где C_j ($j = \overline{1,\,5}$) - множество значений $j-$го параметра модели криптосистемы в соответствии с многокритериальной классификацией, описанной в [18]:

C_1 - по доступности информации о криптоалгоритме;

C_2 - по количеству ключей;

C_3 - по стойкости криптоалгоритма;

C_4 - по используемым средствам;

C_5 - по наличию сертификата;

Каждая модель $\vec{c} \in \mathrm{C}$ представляет собой вектор $\left(c_1, c_2, \ \dots \ , c_5\right)$, где $c_j \in C_j$, $j = \overline{1,\,5}$; мощность множества моделей криптосистем $|\ \mathrm{C}\ | \leq \prod_{j=1}^{5} |\ C_j\ |$.

При дальнейшем изложении для краткости слово «модель» применительно к модели атаки, модели злоумышленника и модели криптосистемы будем опускать.

С каждой атакой будем связывать значение риска, вычисляемое по общеизвестной формуле на основе двух факторов – вероятности происшествия и тяжести возможных последствий:

Риск = Влияние · Вероятность

Обозначим через $\Re : \mathrm{A} \times \mathrm{B} \times \mathrm{C} \to [0\,;\,1]$ функцию, задающую уровень риска, связанного с атакой $\vec{a} \in \mathrm{A}$ в условиях, когда она может быть применена злоумышленником $\vec{b} \in \mathrm{B}$ для взлома криптосистемы $\vec{c} \in \mathrm{C}$.

Пусть $\mathrm{I} : \mathrm{C} \times \mathrm{A} \to [0\,;\,1]$ - функция влияния (от англ. *impact* – влияние, воздействие). Под влиянием мы будем понимать степень ущерба от применения атаки $\vec{a} \in \mathrm{A}$ к криптосистеме $\vec{c} \in \mathrm{C}$.

Пусть $\mathrm{P} : \mathrm{B} \times \mathrm{A} \to [0\,;\,1]$ - вероятность того, что злоумышленник $\vec{b} \in \mathrm{B}$ предпримет атаку $\vec{a} \in \mathrm{A}$, т.е. обладает ресурсами для ее осуществления и сочтет эту атаку целесообразной.

Тогда функция риска $\Re$ выражается следующим образом:

$$\Re(\vec{a}, \vec{b}, \vec{c}) = \mathrm{I}(\vec{c}, \vec{a}) \cdot \mathrm{P}(\vec{b}, \vec{a})$$

Определим функцию $\mathrm{I}(\vec{c}, \vec{a})$. Для этого рассмотрим семейство функций $\mathrm{I}_{gh} : C_g \times A_h \to \mathbb{R}_+$, $g = \overline{1,5}$, $h = \overline{1,8}$, где $\mathbb{R}_+$ - множество неотрицательных действительных чисел. Здесь функция I_{gh} задает уровень взаимного влияния параметра криптосистемы c_g и параметра атаки a_h:

- $\mathrm{I}_{gh}(c, a) = 0$, если атака со значением параметра $a \in A_h$ не применима к криптосистеме со значением параметра $c \in C_g$;
- $0 < \mathrm{I}_{gh}(c, a) < 1$, если значение параметра криптосистемы $c \in C_g$ снижает вероятность успешного применения атаки со значением параметра $a \in A_h$;
- $\mathrm{I}_{gh}(c, a) = 1$, если значение параметра криптосистемы $c \in C_g$ не влияет на применимость атаки с параметром $a \in A_h$;
- $\mathrm{I}_{gh}(c, a) > 1$, если значение параметра криптосистемы $c \in C_g$ указывает на то, что атака с параметром $a \in A_h$ применима для ее взлома.

Уровень взаимного влияния параметров криптосистемы и атаки определяется на основе экспертных оценок.

Обозначим через $\overline{\mathrm{I}_{gh}} : C_g \times A_h \to [0;\,1]$ нормированную функцию:

$$\overline{\mathrm{I}_{gh}}(c, a) = \frac{\mathrm{I}_{gh}(c, a)}{\sum\limits_{\xi \in C_g} \mathrm{I}_{gh}(\xi, a)}$$

Тогда уровень ущерба от применения атаки $\vec{a} \in \mathrm{A}$ к криптосистеме $\vec{c} \in \mathrm{C}$ вычисляется по следующей формуле:

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

где атака и криптосистема заданы параметрами $\left(a_1, a_2, \ \dots \ , a_8\right)$ и $\left(c_1, c_2, \ \dots \ , c_5\right)$ соответственно. Заметим, что уровень влияния всех параметров криптосистемы на

применимость атаки с заданным значением h-го параметра в этой формуле вычисляется по мультипликативному критерию: $\prod_{g=1}^{5} \overline{\mathrm{I}_{gh}}(c_g, a_h)$. Если значение хотя бы одного из параметров криптосистемы противоречит возможности применения атаки, то результатом оценки применимости атаки к криптосистеме будет нулевое значение, что соответствует нулевому уровню ущерба от атаки.

Определим функцию $\mathrm{P}(\vec{b}, \vec{a})$. Для этого рассмотрим семейство функций $\mathrm{P}_{th} : B_t \times A_h \to \mathbb{R}_+$, $t = \overline{1,6}$, $h = \overline{1,8}$. Здесь функция P_{th} задает уровень взаимного влияния параметра злоумышленника b_t и параметра атаки a_h:

- $\mathrm{P}_{th}(b,a) = 0$, если злоумышленник со значением параметра $b \in B_t$ ни при каких обстоятельствах не будет использовать атаку со значением параметра $a \in A_h$;
- $0 < \mathrm{P}_{th}(b,a) < 1$, если значение параметра злоумышленника $b \in B_t$ снижает вероятность использования атаки со значением параметра $a \in A_h$;
- $\mathrm{P}_{th}(b,a) = 1$, если значение параметра злоумышленника $b \in B_t$ не влияет на вероятность использования атаки со значением параметра $a \in A_h$;
- $\mathrm{P}_{th}(b,a) > 1$, если злоумышленник со значением параметра $b \in B_t$ с большой вероятностью будет использовать атаку со значением параметра $a \in A_h$.

Уровень взаимного влияния параметров злоумышленника и атаки также определяется экспертами.

Обозначим через $\overline{\mathrm{P}_{th}} : B_t \times A_h \to [0;\, 1]$ нормированную функцию:

$$\overline{\mathrm{P}_{th}}(b,a) = \frac{\mathrm{P}_{th}(b,a)}{\sum_{\beta \in B_t} \mathrm{P}_{th}(\beta,a)}$$

Тогда вероятность того, что злоумышленник $\vec{b} \in \mathrm{B}$ предпримет атаку $\vec{a} \in \mathrm{A}$, вычислим по формуле:

$$\mathrm{P}(\vec{a},\vec{b}) = \min_{h=\overline{1,8}} \prod_{t=\overline{1,6}} \overline{\mathrm{P}_{th}}(b_t, a_h)$$

где атака и злоумышленник заданы параметрами $\left(a_1,\, a_2,\, \ldots\, ,\, a_8\right)$ и $\left(b_1,\, b_2,\, \ldots\, ,\, b_6\right)$ соответственно.

Таким образом, общая формула для определения уровня риска, связанного с применением атаки $\vec{a} \in \mathrm{A}$ в условиях, когда эта атака может быть применена злоумышленником $\vec{b} \in \mathrm{B}$ для взлома криптосистемы $\vec{c} \in \mathrm{C}$, имеет вид:

$$\Re(\vec{a},\vec{b},\vec{c}) =$$

$$= \min_{h=\overline{1,8}} \prod_{g=\overline{1,5}} \overline{\mathrm{I}_{gh}}(c_g, a_h) \cdot \min_{h=\overline{1,8}} \prod_{t=\overline{1,6}} \overline{\mathrm{P}_{th}}(b_t, a_h) \cdot$$

Будем считать, что криптосистема $\vec{c} \in \mathrm{C}$ подвержена атаке $\vec{a} \in \mathrm{A}$ в условиях, когда ей угрожает злоумышленник $\vec{b} \in \mathrm{B}$, если $\Re(\vec{a},\vec{b},\vec{c}) > \theta$, т.е. связанный с ней уровень риска превышает заданное пороговое значение θ, где $\theta \in [0;\, 1]$. Допустимый уровень риска θ является настраиваемым параметром модели угроз криптосистемы. Значение θ задается с учетом двух критериев:

- критичности защищаемых данных;
- временных и других ресурсов, доступных специалисту, который осуществляет аудит системы.

В общем случае:

- Криптосистема может включать несколько подсистем (например, генератор ключей и симметричный шифратор), к каждой из которых применим свой набор атак;
- На криптосистему может нападать несколько злоумышленников.

Множество атак, которым подвержена криптосистема, состоящая из подсистем $\vec{c} \in \mathrm{C}'$ ($\mathrm{C}' \subseteq \mathrm{C}$), в условиях, когда ей угрожают злоумышленники $\vec{b} \in \mathrm{B}'$ ($\mathrm{B}' \subseteq \mathrm{B}$), будем определять по формуле $\Lambda = \bigcup_{\vec{b} \in B'} \bigcup_{\vec{c} \in C'} \lambda(\vec{b},\, \vec{c})$, где $\lambda(\vec{b},\vec{c}) = \left\{ \vec{a} \in \mathrm{A} :\ \Re(\vec{a},\vec{b},\vec{c}) > \theta \right\}$ при заданном уровне риска. Для оценки защищенности криптосистемы необходимо с использованием инструментальных средств оценить ее способность противостоять атакам, входящим в множество Λ.

В описанной математической модели сделаны следующие допущения:

- Не учитывается зависимость параметров атаки от сочетания параметров криптосистемы, хотя влияние каждого параметра принимается во внимание;
- Не учитывается возможность совместных действий со стороны взломщиков различных типов, хотя можно задать

модель нападения со стороны однородного коллектива злоумышленников.

Исправление модели с учетом указанных допущений привело бы к ее значительному усложнению. Вопрос о том, насколько эти допущения снижают точность моделирования угроз безопасности, подлежит дальнейшим исследованиям.

На данный момент обнаружены две проблемы, связанные с практической реализацией разработанной модели в виде программного инструментария для аудитора:

- Получение экспертных оценок взаимного влияния параметров криптосистемы и атаки, а также злоумышленника и атаки;
- Поддержание базы оценок в актуальном состоянии, т.к.
  - с ростом вычислительных мощностей, изменением цен на аппаратные и программные средства и под влиянием других факторов уровень взаимного влияния параметров может меняться;
  - с появлением новых видов атак может возникнуть необходимость дополнения разработанных классификационных схем новыми критериями, что потребует введения новых зависимостей для соответствующих параметров моделей.

5. Расчет эффективности капитальных вложений в использование СКЗИ

На основании анализа преимуществ и недостатков методом оценки эффективности инвестиций в средства обеспечения ИБ (см. табл.1) был сделан вывод, что оптимальным является *метод дисконтированных показателей* [19], позволяющий получить наиболее полное представление о целесообразности капитальных вложений, хотя и требующий много времени и усилий на расчет экономических показателей.

Определим денежные потоки, связанные с использованием СКЗИ, за период t (где t = 0, 1, 2…. T - периоды, T – горизонт расчета).

Затраты $Cost_t$ на приобретение, установку и эксплуатацию СКЗИ могут быть определены очень точно, т.к. основной объем затрат составляет оплата труда персонала службы безопасности.

С защищаемой информацией связаны значения дохода $Profit_t$ и ущерба $Loss_t$ от НСД к защищаемой информации в течение указанного промежутка времени t. Пусть результаты оценки способности криптосистемы противостоять атакам, представляющих для нее угрозу (см. п. 4) с использованием инструментальных средств показали, что с вероятностью P_t в t-м периоде злоумышленник получит доступ к защищаемой информации. Тогда математическое ожидание дохода R_t, связанного с использованием оцениваемой СКЗИ, вычисляется по формуле:

$$R_t = -Cost_t + Profit_t \cdot (1 - \mathrm{P}_t) - Loss_t \cdot \mathrm{P}_t$$

На основании этих данных о притоках и оттоках денежных средств вычисляются финансово-экономические показатели эффективности инвестиций в криптосистему и делаются выводы о ее соответствии потребностям организации.

6. Анализ разработанной методики

К достоинствам разработанной методики оценки эффективности криптосистем можно отнести следующее:

- В основе методики лежит комплексный подход к оценке рисков, основанный на

Методика оценки	Преимущества	Недостатки
Коэффициент возврата инвестиций	• Показатель, понятный финансистам	• Отсутствие достоверных методов расчета в области ИТ • «Статичный» показатель
Совокупная стоимость владения	• Позволяет оценить целесообразность реализации проекта на основании оценки только затрат • Предполагает оценку затрат на различных этапах всего жизненного цикла 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 денежных средств, связанные с реализацией проекта	• Сложность расчета

Таблица 1 - Сравнительный анализ методов оценки эффективности инвестиций в средства обеспечения ИБ

формализованном пятиэтапном процессе оценки эффективности криптосистемы и математической модели угроз.

- Методика является универсальной и подходит для организаций различного масштаба как правительственного, так и коммерческого сектора.
- Методика помогает провести анализ рисков, сочетающий количественные и качественные методы анализа, и сделать обоснованный выбор мер и средств криптографической защиты.
- Методика позволяет провести экономическое обоснование расходов организации на обеспечение информационной безопасности и непрерывности бизнеса с использованием СКЗИ.
- Методика позволяет оценить не только риски, связанные с защищаемыми информационными ресурсами, но и выгоду, которую может принести внедрение СКЗИ.

К недостаткам разработанной методики можно отнести следующее:

- Использование методики требует специальной подготовки и высокой квалификации аудитора.
- Методика в большей степени подходит для аудита уже существующих криптосистем, находящихся на стадии эксплуатации, чем для криптосистем, находящихся на стадии разработки.
- Аудит с использованием разработанной методики - достаточно трудоемкий процесс, который может потребовать месяцев работы специалиста.
- Использование методики предполагает наличие экспертов, способных дать достоверные оценки объема потерь от реализации угроз ИБ;
- На данный момент программное обеспечение, автоматизирующее процесс построения модели угроз на основе данных об особенностях реализации исследуемой криптосистемы и типах потенциальных злоумышленников, находится на стадии разработки.

7. Список литературы

[1] ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

[2] Яковлев А.В., Безбогов А.А., Родин В.В., Шамкин В.Н. Криптографическая защита информации: учебное пособие / Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. – 140 с.

[3] Иванов В.П. Математическая оценка защищенности информации от несанкционированного доступа // "Специальная техника". 2004, N 1. -с. 58-64.

[4] Brassard J. Modern Cryptologyy. Springer-Verlag, Berlin - Heidelberg, 1988. - 107 p. (Русский перевод: Брассар Ж. Современная криптология. Полимед, 1999. 176 с.)

[5] Kerckhoffs A. La cryptographie militaire // Journal des sciences militaires, vol. IX. P. 5-38, Jan. 1883, (P. 161-191, Feb. 1883).

[6] Savelieva A. Formal methods and tools for evaluating cryptographic systems security // St. Petersburg, ISP RAS, In Proceedings of the Second Spring Young Researchers Colloquium on Software Engineering (SYRCoSE'2008), 2008, Vol 1. P. 33-36.

[7] Schneier B. Modeling security threats // Dr. Dobb's Journal, December, 1999.

[8] Баричев С.Г. Основной вопрос криптографии // Chief Inforamtion Officer – руководитель информационной службы. #5 (37), 2005, с. 93-95.

[9] Куканова Н. Методы и средства анализа рисков и управление ими в ИС // Byte/Россия. - 2005. - № 12. - С. 69-73.

[10] Куканова Н. Современные методы и средства анализа и управления рисками информационных систем компаний // Опубликовано: http://www.dsec.ru/about/articles/ar_compare/ 2006.03.17

[11] CRAMM V Official website // Siemens Enterprise Communications Limited 2006. Available at: www.cramm.com

[12] RiskWatch Official website // RiskWatch, Inc. Available at: http://www.riskwatch.com/

[13] Digital Security: ГРИФ. Система анализа и управления информационными рисками // Digital Security, 2002-2008. Опубликовано: http://www.dsec.ru/products/grif/

[14] Авдошин С.М., Савельева А.А. Инструментальные средства криптоанализа асимметричных шифров. - М.: ВНТИЦ, 2008. - №50200800603.

[15] Авдошин С.М., Савельева А.А. Инструментальные средства криптоанализа асимметричных шифров. Свидетельство о государственной регистрации в Реестре программ для ЭВМ № 2005612258 от 22.05.08.

[16] Ростовцев А.Г., Михайлова Н.В. Методы криптоанализа классических шифров // 1998. Опубликовано: http://crypto.hotbox.ru/download/cryptoan.zip

[17] Авдошин С.М., Савельева А.А. Криптоанализ: современное состояние и перспективы развития. Новые технологии; М.: Машиностроение, 2007. - 24 с. - (Библиотечка журнала "Информационные технологии"; Приложение к журналу "Информационные технологии";№ 3)

[18] Авдошин С.М., Савельева А.А. Проблемы оценки криптозащищенности информационных систем // «Новые информационные технологии». Тезисы докладов XVI Международной студенческой школы-семинара - М.: МИЭМ, 2008. С. 15-29.

[19] Старик Д.Э. Расчеты эффективности инвестиционных проектов. М.: Финстатинформ, 2001.