

МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ, ЗАЩИЩЕННЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ

Авдошин С.М., Савельева А.А.

ГУ - ВШЭ

MODELING SECURITY THREATS TO INFORMATION ASSETS PROTECTED BY MEANS OF CRYPTOGRAPHIC TOOLS<sup>1</sup>

Avdoshin S.M., Savelieva A.A.

In this paper, we introduce a mathematical model of threats for analyzing the security of cryptographic systems based on risk management principles. The model presented here is a part of our approach that also incorporates automatic cryptographic strength verification tools and economic techniques and is designed for providing sound arguments to choose a cryptographic system and for implementing an information security strategy.

Появление криптографии на сотни лет опередило наступление компьютерной эры. Однако до появления и распространения вычислительной техники, когда обработка информации велась вручную, а сделки сопровождались «бумажной» документацией, использование криптографических методов в основном касалось государственных структур и военных ведомств. В последние десятилетия внедрение средств вычислительной техники в различные сферы бизнеса привело к изменению ситуации, что в большой степени связано с появлением новых методов совершения финансовых транзакций с использованием технологий электронной коммерции. Это привело к разделению понятий «государственной» криптографии (используемой государственными и муниципальными учреждениями и регламентированной стандартами на уровне отдельных стран), а также «коммерческой» криптографии (основными потребителями которой являются финансовые учреждения). С появлением коммерческой криптографии перед специалистами по защите информации встали новые научные, технические и организационные задачи, такие как:

- анализ затрат и выгод на применение криптотехнологий, с учетом расходов на «переучивание» в случае перехода на новые средства криптографической защиты [1];
- построение информационной инфраструктуры, объединяющей компании по всему миру и обеспечивающей совместимость используемых криптографических механизмов [2];
- обеспечение защиты персональных данных, обрабатываемых в информационных системах [1].

В данной работе мы рассматриваем методы и инструменты определения эффективности средств коммерческой криптографии.

Задача оценки эффективности защиты, обеспечиваемой криптосистемой, сводится к выделению подмножества атак, которым может подвергаться система в данном контексте использования, и определению устойчивости системы к этим атакам. Под устойчивостью системы будем понимать ее криптостойкость, то есть способность противостоять атакам криптоаналитика [5]. Для определения эффективности криптосистемы имеет смысл 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, на основании предложенной модели сценария атаки (рисунок 1) построим математическую модель угроз безопасности криптосистемы из трех элементов — *ABC-модель* («А» от англ. *Attack* — атака, «В» от англ. *code-Breaker* — взломщик шифра, «С» от англ. *Cryptosystem* — криптосистема), основываясь на следующих предположениях:

- 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  $A \subseteq A_1 \times A_2 \times \dots \times A_9$  — множество параметрических моделей атак, где  $A_j$  ( $j = \overline{1, 9}$ ) — множество значений  $j$ -го параметра модели атаки, определяющего тип атаки в соответствии с критериями разработанной классификации [4]:

$A_1$  — по доступу к открытому коду;

$A_2$  — по контролю над процессом шифрования;

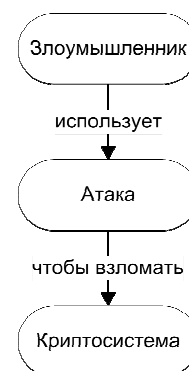


Рис. 1. Модель сценария взлома криптосистемы

<sup>1</sup> Работа выполнена в рамках исследовательского проекта «Исследование и разработка методов оценки эффективности использования криптографических средств защиты информации в сфере бизнеса и финансов», поддержанного государственным грантом № П965 от 27 мая 2010 г.

- $A_3$  — 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;
- $A_9$  — по уровню автоматизации.

Каждая модель  $\vec{a} \in A$  представляет собой вектор  $(a_1, a_2, \dots, a_9)$ , где  $a_j \in A_j$ ,  $j = \overline{1, 9}$ . Заметим, что, поскольку множества значений параметров модели атаки конечны, то мощность множества моделей атак  $|A| \leq \prod_{j=1}^9 |A_j|$ .

Пусть  $B \subseteq B_1 \times B_2 \times \dots \times B_6$  — множество параметрических моделей злоумышленников, где  $B_j$  ( $j = \overline{1, 6}$ ) — множество значений  $j$ -го параметра модели злоумышленника в соответствии с критериями разработанной и описанной в [4] 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  $\vec{b} \in B$  задана в виде вектора  $(b_1, b_2, \dots, b_6)$ , где  $b_j \in B_j$ ,  $j = \overline{1, 6}$ ,  $|B| \leq \prod_{j=1}^6 |B_j|$ .

Пусть  $C \subseteq C_1 \times C_2 \times \dots \times C_6$  — множество параметрических моделей криптосистем, где  $C_j$  ( $j = \overline{1, 6}$ ) — множество значений  $j$ -го параметра модели криптосистемы в соответствии с многокритериальной классификацией, описанной в [4]:

- $C_1$  — 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;
- $C_6$  — по типу хранилища ключа.

Каждая модель  $\vec{c} \in C$  представляет собой вектор  $(c_1, c_2, \dots, c_6)$ , где  $c_j \in C_j$ ,  $j = \overline{1, 6}$ ; мощность множества моделей криптосистем  $|C| \leq \prod_{j=1}^6 |C_j|$ .

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 как произведение вероятности происшествия и тяжести возможных последствий. Обозначим через  $\mathfrak{R} : A \times B \times C \rightarrow [0; 1]$  функцию, задающую уровень риска, связанного с применением атаки  $\vec{a} \in A$  в условиях, когда эта атака может быть применена злоумышленником  $\vec{b} \in B$  для взлома криптосистемы  $\vec{c} \in C$ .

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

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

Тогда функция риска  $\mathfrak{R}$  выражается следующим образом:

$$\mathfrak{R}(\vec{a}, \vec{b}, \vec{c}) = I(\vec{c}, \vec{a}) \cdot P(\vec{b}, \vec{a}) .$$

Определим функцию  $I(\vec{c}, \vec{a})$ . Для этого рассмотрим семейство функций  $I_{gh} : C_g \times A_h \rightarrow \mathbb{R}_+$ ,  $g = \overline{1,6}$ ,  $h = \overline{1,9}$ , где  $\mathbb{R}_+$  — множество неотрицательных действительных чисел. Здесь функция  $I_{gh}$  задает уровень взаимного влияния параметра криптосистемы  $c_g$  и параметра атаки  $a_h$ :

- $I_{gh}(c, a) = 0$ , если атака со значением параметра  $a \in A_h$  не применима к криптосистеме со значением параметра  $c \in C_g$ ;
- $0 < I_{gh}(c, a) < 1$ , если значение параметра криптосистемы  $c \in C_g$  снижает вероятность успешного применения атаки со значением параметра  $a \in A_h$ ;
- $I_{gh}(c, a) = 1$ , если значение параметра криптосистемы  $c \in C_g$  не влияет на применимость атаки с параметром  $a \in A_h$ ;
- $I_{gh}(c, a) > 1$ , 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  $\overline{I}_{gh} : C_g \times A_h \rightarrow [0; 1]$  нормированную функцию:

$$\overline{I}_{gh}(c, a) = \frac{I_{gh}(c, a)}{\sum_{\xi \in C_g} I_{gh}(\xi, a)}.$$

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

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

где атака и криптосистема заданы параметрами  $(a_1, a_2, \dots, a_8)$  и  $(c_1, c_2, \dots, c_6)$  соответственно. Заметим, что уровень влияния всех параметров криптосистемы на применимость атаки с заданным значением  $h$ -го параметра в этой формуле вычисляется по мультипликативному критерию:  $\prod_{g=1}^6 \overline{I}_{gh}(c_g, a_h)$ . 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  $P(\vec{b}, \vec{a})$ . Для этого рассмотрим семейство функций  $P_{th} : B_t \times A_h \rightarrow \mathbb{R}_+$ ,  $t = \overline{1,6}$ ,  $h = \overline{1,9}$ . Здесь функция  $P_{th}$  задает уровень взаимного влияния параметра злоумышленника  $b_t$  и параметра атаки  $a_h$ :

- $P_{th}(b, a) = 0$ , если злоумышленник со значением параметра  $b \in B_t$  ни при каких обстоятельствах не будет использовать атаку со значением параметра  $a \in A_h$ ;
- $0 < P_{th}(b, a) < 1$ , если значение параметра злоумышленника  $b \in B_t$  снижает вероятность использования атаки со значением параметра  $a \in A_h$ ;
- $P_{th}(b, a) = 1$ , если значение параметра злоумышленника  $b \in B_t$  не влияет на вероятность использования атаки со значением параметра  $a \in A_h$ ;
- $P_{th}(b, a) > 1$ , 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  $\overline{P}_{th} : B_t \times A_h \rightarrow [0; 1]$  нормированную функцию:

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

Тогда вероятность того, что злоумышленник  $\vec{b} \in B$  предпримет атаку  $\vec{a} \in A$ , заданную параметрами  $(a_1, a_2, \dots, a_9)$ , вычислим по формуле:

$$P(\vec{a}, \vec{b}) = \min_{h=\overline{1,9}} \prod_{t=\overline{1,6}} \overline{P}_{th}(b_t, a_h),$$

где атака и злоумышленник заданы параметрами  $(a_1, a_2, \dots, a_9)$  и  $(b_1, b_2, \dots, b_6)$  соответственно.

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

$$\mathfrak{R}(\vec{a}, \vec{b}, \vec{c}) = \min_{h=1,9} \prod_{g=1,6} \overline{I}_{gh}(c_g, a_h) \cdot \min_{h=1,9} \prod_{t=1,6} \overline{P}_{th}(b_t, a_h).$$

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

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

В общем случае:

1. Криптосистема может включать несколько подсистем (например, генератор ключей и асимметричный шифратор), к каждой из которых применим свой набор атак.
2. На криптосистему может напасть несколько злоумышленников.

Множество атак, которым подвержена криптосистема, состоящая из подсистем  $\vec{c} \in C'$  ( $C' \subseteq C$ ), в условиях, когда ей угрожают злоумышленники  $\vec{b} \in B'$  ( $B' \subseteq B$ ), будем определять по формуле  $\Lambda = \bigcup_{\vec{b} \in B'} \bigcup_{\vec{c} \in C'} \lambda(\vec{b}, \vec{c})$

, где  $\lambda(\vec{b}, \vec{c}) = \{ \vec{a} \in A : \mathfrak{R}(\vec{a}, \vec{b}, \vec{c}) > \theta \}$  при заданном уровне риска. Для оценки защищенности криптосистемы необходимо с использованием инструментальных средств оценить ее способность противостоять атакам, входящим в множество  $\Lambda$ .

В математической модели, описанной выше, сделаны следующие допущения:

1. Не учитывается зависимость параметров атаки от сочетания параметров криптосистемы, хотя влияние каждого параметра принимается во внимание.
2. Не учитывается возможность совместных действий со стороны взломщиков различных типов, хотя можно создать модель нападения со стороны однородного коллектива злоумышленников.

Исправление указанных допущений привело бы к значительному усложнению модели. Вопрос о том, насколько эти допущения снижают точность результатов оценки, подлежит дальнейшим исследованиям.

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

1. Получение экспертных оценок взаимного влияния параметров криптосистемы и атаки, а также злоумышленника и атаки.
2. Поддержание базы оценок в актуальном состоянии:
  - 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.

Важно отметить, что разработанная классификационная схема для построения моделей атак на алгоритмы шифрования с небольшими модификациями применима и для моделирования атак на криптопротоколы. Возможность использования ABC-модели угроз для комплексного исследования криптосистемы является важной, так как вопрос совместного функционирования криптопротоколов и шифров в рамках одной криптосистемы, как показано в [3], до сих пор был мало изучен.

#### СПИСОК ЛИТЕРАТУРЫ

1. Hoffman L.J. Clipping Clipper // Communications of the ACM, Volume 36 Issue 9, September 1993.
2. Turner G.W. Commercial Cryptography at the Crossroads. Information Systems Security 1: 34–42, 1992.
3. Verma R. Protocol Specification and Verification [Электронный ресурс]. Lectures on COSC 6397 — Information Assurance. University of Houston, 2006. URL [www2.cs.uh.edu/~rmverma/M2L1.ppt](http://www2.cs.uh.edu/~rmverma/M2L1.ppt) (дата обращения: 22.08.10).
4. Авдошин С.М., Савельева А.А. О новом подходе к проблеме анализа эффективности криптосистем // Информационные технологии. — 2009. — № 8. — С. 2–9.
5. Ростовцев А.Г., Михайлова Н.В. Методы криптоанализа классических шифров [Электронный ресурс] — Сайт [www.realcoding.net](http://www.realcoding.net), 1998. URL: <http://www.realcoding.net/articles/metody-kriptoanaliza-klassicheskikh-shifrov.html> (дата обращения: 22.08.10).