# ОБ ОЦЕНКЕ РИСКОВ ПРИ АНАЛИЗЕ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ ЗАЩИТЫ ИНФОРМАЦИИ

**А. Ю. Ермакова[1], А. Б. Лось[2]**

*[1]Российский технологический университет МИРЭА, Москва, Россия*
*[2]Национальный исследовательский университет «Высшая школа экономики», Москва, Россия*
E-mail: a.alla1105@yandex.ru , alexloss2011@mail.ru

Настоящая статья посвящена вопросам применения методов оценки рисков к исследованию эффективности алгоритмов защиты информации.

Под алгоритмами защиты информации при этом понимаются алгоритмы преобразования информации по определенному правилу, зависящему от секретного ключа. Сюда же относятся и алгоритмы аутентификации, применяющие секретные ключи, а также различные парольные системы. Предложен метод оценки эффективности указанных алгоритмов, основанный на подсчете возникающих рисков при компрометации секретного ключа. Предложен также подход к анализу данных алгоритмов, основанный на оценке времени, в течение которого будет сохраняться их эффективность. Данный подход основан на построении прогнозной модели увеличения производительности средств вычислительной техники. Проведены численные расчеты, иллюстрирующие предлагаемый подход.

# ON RISK ASSESSMENT WHEN ANALYZING THE EFFECTIVENESS OF INFORMATION PROTECTION ALGORITHMS

**A. Y. Ermakova, A. B. Los**

This article is devoted to the application of risk assessment methods to the study of the effectiveness of information security algorithms. Information protection algorithms are understood to be algorithms for converting information according to a certain rule that depends on the secret key. This also includes authentication algorithms that use secret keys, as well as various password systems. A method for evaluating the effectiveness of these algorithms is proposed, based on calculating the risks arising from compromising the secret key. An approach to the analysis of these algorithms is also proposed, based on an estimate of the time during which their effectiveness will be maintained. This approach is based on the construction of a predictive model for increasing the productivity of computer equipment. Numerical calculations illustrating the proposed approach are carried out.

## Введение

Настоящая статья посвящена вопросам применения методов оценки рисков к исследованию эффективности алгоритмов защиты информации.

Под алгоритмами защиты информации при этом понимаются алгоритмы преобразования информации по определенному правилу, зависящему от секретного ключа. Сюда же относятся и алгоритмы аутентификации, применяющие секретные ключи, а также различные парольные системы. В работе предложен метод оценки эффективности указанных алгоритмов, основанный на

подсчете возникающих рисков при компрометации секретного ключа, а также подход к анализу данных алгоритмов, основанный на оценке времени, в течение которого будет сохраняться их эффективность. Данный подход основан на построении прогнозной модели увеличения производительности средств вычислительной техники.

В последнее время подход, основанный на оценке рисков, широко используется в вопросах оценки уровня защищенности информационных систем (ИС) и в вопросах разработки политики безопасности организации. Данный подход закреплен в стандартах по информационной безопасности, как отечественных, так и зарубежных, хотя в последней версии международного стандарта (ИСО 27000 [1]) отсутствует количественная характеристика риска и примеры его вычисления.

Сутью данного подхода является первоначальное вычисление функции рисков:

$$R=\sum_{i=1}^{n} p(y_i)\cdot u_i, \tag{1}$$

где $\{y_i\}$ множество актуальных угроз ИС, $p(y_i)$ – вероятность реализации злоумышленником угрозы $y_i$, $u_i$ – величина потерь от успешного осуществления соответствующей угрозы, $i=1,2,...,n$.

В дальнейшем устанавливается граница максимально возможных потерь $R_0$ и, при выполнении условия:

$$R \le R_0 \tag{2}$$

делается вывод о защищенности системы.

Далее в работе изучается возможность применения данного подхода к оценке эффективности алгоритмов защиты информации в части методов определения секретного ключа, сложность нахождения которого обеспечивает защиту передаваемой информации. Данную методику можно использовать и в других задачах защиты информации, в том числе, в задачах применения аналогичных алгоритмов для обеспечения целостности информации и подтверждения подлинности сообщений.

Для дальнейших исследований будем считать, что основной угрозой при применении алгоритмов защиты является угроза определения атакующим истинного секретного ключа, на котором произведено преобразование исходного сообщения или который является параметром, позволяющим получить доступ к ресурсам ИС. В этом случае, очевидно, возникает угроза компрометации всего передаваемого сообщения, его части или угроза доступа злоумышленника к ресурсам системы.

В рассматриваемой ситуации функция риска (1) принимает вид:

$$R = P_{кл} \times U, \tag{3}$$

где $P_{кл}$ – вероятность определения секретного ключа, $U$ – ущерб от компрометации сообщения (или аутентификационного параметра системы), а условие эффективности алгоритма защиты имеет вид:

$$P_{кл} \times U \le R_0 \times \pi_0, \tag{4}$$

где $\pi_0$ – доля компрометированной информации, при которой атака считается успешной.

При применении риск – ориентированного подхода важную роль играет вопрос о размерах потерь $U$ при успешной реализации угрозы – компрометации ключа и, соответственно, компрометации всего сообщения или его части ([2]). Нетрудно видеть, что величина $U$, в значительной степени, будет зависеть от условий применения конкретного алгоритма и ценности защищаемой информации. В этом случае эффективность алгоритма становится зависимой от этих условий и возникает необходимость ее оценки при каждом применении такого алгоритма. Не меньшей проблемой становится задача определения стоимости защищаемой информации и границы для максимально возможного уровня потерь. Заметим, что авторам ничего неизвестно об исследованиях в этой области и каких-либо обоснованных решениях. Тем не менее, при возникновении такой задачи, наличии обоснованных данных о ценности защищаемой информации и уровне максимально возможных потерь, при исследовании эффективности алгоритмов защиты можно воспользоваться функцией риска (3). Еще большей проблемой становится задача установления потерь при получении злоумышленником несанкционированного доступа к ресурсам информационной системы. В этом случае количество различных ситуаций, в которых возможно нанесение злоумышленником ущерба информационной системе и организации в целом многократно возрастает.

В практических ситуациях, создатели и исследователи алгоритмов защиты информации придерживаются вполне обоснованного мнения, что эффективность алгоритмов является некоторой объективной характеристикой и не должна зависеть от условий эксплуатации. При этом для защиты каналов связи с более ценной информацией или важных информационных систем следует использовать более эффективные алгоритмы защиты.

Таким образом, в рассматриваемой ситуации при применении риск – ориентированного подхода предлагается отойти от вопроса потерь при успешной реализации атаки. В частности, предлагается считать, что величина ущерба $U$ в случае определения секретного ключа равна максимальному значению ущерба $R_0$. В этом случае, очевидно, граница риска увеличивается и создается определенный запас прочности рассматриваемого алгоритма защиты.

Условие эффективности алгоритма защиты при этом имеет вид:

$$P_{кл} \leq \pi_0 . \qquad (5)$$

Заметим, что эффективность алгоритма защиты определяется наименее сложным (трудоемким) из известных методов нахождения секретного ключа. В связи с этим алгоритм защиты будет эффективным, если наименее сложный метод определения ключа удовлетворяет условию (5).

Однако, очевидно, что такой подход не отвечает на вопрос в течение, какого времени для данного алгоритма будет выполняться условие (5), то есть, в течение какого времени алгоритм защиты будет оставаться эффективным.

С целью оценки времени, в течение которого алгоритм защиты будет оставаться эффективным предлагается ввести аналитическую зависимость веро-

ятности определения секретного ключа $P_{кл}$ от времени $t$:

$$P_{кл} = P_{кл}\ (t). \qquad (6)$$

Такой подход для анализа защищенности информационных систем ранее предлагался в работе [3] и получил дальнейшее развитие в работах [4] -[7].

Заметим, что как правило, функция $P_{кл}\ (t)$ является неубывающей функцией $t$. Это связано с тем, что для большинства эффективных алгоритмов защиты процедура определения секретного ключа, как правило, состоит в последовательном переборе его вариантов и осуществляется на современных вычислительных комплексах, производительность которых монотонно возрастает с течением времени. При этом очевидно, что вероятность определения истинного ключа также возрастает с течением времени.

Путем решения уравнения

$$P_{кл}\ (t) = \pi_0 \qquad (7)$$

относительно неизвестной величины $t$ можно получить оценку промежутка времени, в течение которого алгоритм защиты будет эффективным. Очевидно, что чем больше временной промежуток, в течение которого выполняется соотношение (5), тем эффективнее алгоритм информационной защиты.

Далее в работе исследуется типовая ситуация проведения анализа алгоритмов защиты и для нее оцениваются значения риска и время, в течение которого сохраняется эффективность алгоритма. Аналогичный подход может быть применен к исследованию и других методов определения секретного ключа алгоритмов информационной защиты и аутентификационных параметров ИС, а также их эффективности.

Пусть некоторый алгоритм информационной защиты имеет в общей сложности $K$ различных вариантов секретных ключей и аналитик, исследующий данный алгоритм не располагает информацией о вероятности использования конкретного секретного ключа сообщения. Другими словами, предполагается, что все варианты ключей алгоритма, которые могут быть использованы для преобразования исходного сообщения, равновероятны, а длина самого сообщения достаточна для однозначного определения истинного варианта секретного ключа ([2]).

В этом случае, очевидно, выбор вариантов ключа для опробования осуществляется по урновой схеме без возвращения из общего множества ключей. Без ограничения общности будем предполагать, что опробование варианта ключа осуществляется за одну операцию, которую можно назвать элементарной, и положим $Q_0$ - количество элементарных операций, совершаемых вычислительной системой в единицу времени, например, в секунду.

Вначале рассмотрим более простую ситуацию, когда производительность вычислительной системы не изменяется с течением времени. Обозначим через $p(T)$ вероятность определения истинного варианта секретного ключа алгоритма за время $T$. Нетрудно видеть, что величина $p(T)$ имеет вид:

$$p(T) = \sum_{k=1}^{N(T)} \frac{1}{K} = \frac{1}{K} \cdot N(T), \qquad (8)$$

где $N(T) = T \cdot Q_0$ – производительность вычислительной системы, то есть, число

вариантов ключей, которое опробует система за время *T*.

Из соотношения (8) следует равенство:

$$p(T) = \frac{Q_0 \cdot T}{K}.$$

Принимая во внимание соотношение (7), находим условие для вычисления времени *T*, в течение которого алгоритм будет эффективным по отношению к переборному методу поиска секретного ключа:

$$\frac{Q_0 \cdot T}{K} = \pi_0 . \qquad (9)$$

Из выражения (9) находим значение времени *T*, в течение которого алгоритм информационной защиты сохраняет эффективность относительно метода перебора секретных ключей:

$$T = \frac{K \cdot \pi_0}{Q_0}.$$

В табл. 1 приведены данные расчетов по оценке времени, в течение которого сохраняется эффективности алгоритмов защиты, полученные без учета увеличения производительности вычислительных средств.

*Таблица 1*

**Время сохранения эффективности алгоритма относительно метода перебора секретных ключей**

| № | Длина ключа (бит) | Общее число ключей | Время (года) |
|---|---|---|---|
| 1 | 128 | $2^{128} \sim 10^{38}$ | $10^7$ |
| 2 | 256 | $2^{256} \sim 10^{77}$ | $10^{45}$ |
| 3 | 512 | $2^{512} \sim 10^{153}$ | $10^{122}$ |

Далее для оценки эффективности алгоритма защиты информации исследуем возможность учета увеличения производительности средств вычислительной техники. С этой целью воспользуемся результатами работы [4]. В данной работе предложен метод прогнозирования состояний динамического процесса по начальным данным путем построения непрерывной аппроксимирующей функции, сохраняющей на прогнозируемом участке статистические характеристики исследуемого процесса. В работе [4] по данным за 20 прошлых лет построена прогнозная функция увеличения производительности вычислительных средств. Результаты разработки методов прогнозирования состояний динамической системы, кроме того, изложены ранее в работах [5]- [7].

Применяя полученные в работе [4] результаты, находим условие для оценки времени *T* (в годах), в течение которого алгоритм защиты информации будет эффективным относительно метода полного перебора вариантов секретного ключа:

$$\frac{1}{K} \cdot \sigma \cdot T \cdot \beta \cdot (30+T)^2 \cdot 10^{12} = \pi_0 ,$$

где $\sigma = 3{,}1 \cdot 10^7$ - количество секунд в одном году. В табл. 1 приведены расчеты времени обеспечения стойкости для значения $\pi_0 = 10^{-5}$ и производительности

вычислителя на 2021 год $Q_0 = 1{,}2 \cdot 10^{18}$ оп/сек [8].

В табл. 2 приведены данные расчетов по оценке времени, в течение которого сохраняется эффективности алгоритмов защиты, полученные с учетом увеличения производительности вычислительных средств. Сравнение данных табл. 1 и 2 показывает существенную разницу в оценке времени, в течение которого сохраняется свойство эффективности алгоритмов информационной защиты. При этом можно сделать вывод, что, не учитывая важные факторы, влияющие на безопасность ИС, мы недооцениваем возможные угрозы и рискуем попасть в сложную ситуацию, в том числе понести большие потери.

*Таблица 2*

**Время сохранения эффективности алгоритма относительно метода перебора секретных ключей с учетом увеличения производительности вычислений**

| № | Длина ключа (бит) | Общее число ключей | Время (года) |
|---|---|---|---|
| 1 | 128 | $2^{128} \sim 10^{38}$ | 270 |
| 2 | 256 | $2^{256} \sim 10^{77}$ | $10^{15}$ |
| 3 | 512 | $2^{512} \sim 10^{153}$ | $10^{40}$ |

## Заключение

В работе исследована возможность применения риск – ориентированного подхода к оценке эффективности алгоритмов защиты информации, алгоритмов аутентификации и парольных систем. Рассмотрены общие вопросы применения указанного подхода и предложена методика оценки эффективности указанных алгоритмов с учетом увеличения с течением времени производительности вычислительных средств, применяемых для осуществления атак на данные алгоритмы. Показано, что учет важных факторов, влияющих на безопасность, таких как развитие средств вычислительной техники, может существенным образом повлиять на показатели безопасности информационных систем. Проведенные исследования показывают также, что подход к анализу алгоритмов защиты информации, основанный на оценке рисков, позволяет оценить время, в течение которого исследуемый алгоритм информационной защиты остается эффективным, что позволяет определить условия его применения для надежной защиты информационных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Международный стандарт информационной безопасности ISSO/17799.

2. *Лось А. Б., Нестеренко А. Ю., Рожков М. И.* Криптографические методы защиты информации. Учебник для изучающих компьютерную безопасность, издание 2, исправленное, 2021. 473 с.

3. *Кабанов А. С., Лось А. Б., Трунцев В. И.* Временная модель оценки риска нарушения информационной безопасности // Доклады ТУСУУР. 2012. С. 87-91.

4. *Ермакова А. Ю.* Разработка методов прогнозирования на примере анализа средств вычислительной техники // Промышленные АСУ и контроллеры. 2017. № 1. С.28-34.

5. *Ермакова А. Ю.* Об оценке точности прогнозирования состояния динамической системы методом построения аппроксимирующих функций // Промышленные АСУ и контроллеры. 2018. № 5. С. 36−42.

6. *Ермакова А. Ю. Лось А. Б.* Исследование прогнозных моделей динамической системы на примере прогноза инцидентов информационной безопасности // Компьютерные науки и информационные технологии: сборник статей Междун. науч.-практич. конф. 2018. С. 144−149.

7. *Ермакова А. Ю.* Об одном подходе к оценке защищенности информационной системы на основе анализа инцидентов // Системы высокой доступности. 2018. № 4. С. 32-35.

8.Википедия. Свободная энциклопедия. [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/FLOPS (дата обращения 11.09.2022).