ВЕСТНИК НАЦИОНАЛЬНОГО ИССЛЕДОВАТЕЛЬСКОГО ЯДЕРНОГО УНИВЕРСИТЕТА "МИФИ", 2021, том 10, № 3, с. 239–243

ПРИКЛАДНАЯ МАТЕМАТИКА И ИНФОРМАТИКА

УДК 621.039

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОПТИМИЗАЦИИ ЗАТРАТ НА СИСТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЕВЫХ КАНАЛАХ СВЯЗИ СИСТЕМ УПРАВЛЕНИЯ

© 2021 г. С. Г. Климанов[1], А. В. Крянев[1,*], Н. А. Кудряшов[1]

[1] Национальный исследовательский ядерный университет "МИФИ", Москва, 115409, Россия

**e-mail: AVKryanev@mephi.ru*

Поступила в редакцию 06.07.2021 г.
После доработки 07.07.2021 г.
Принята к публикации 13.07.2021 г.

В настоящей статье рассматривается актуальная задача защиты информации, которая может стать доступной через сетевые каналы связи, от хакерских атак. Эта задача связана с хранением и передачей информации в системах управления отдельными предприятиями и отраслями, в частности электронной промышленности. Для создания системы защиты информации от угроз требуются материальные затраты, величина которых растет с ростом уровня обеспечения защиты информации. В статье предлагается математическая схема определения такого оптимального уровня материальных затрат в систему защиты информации, которая обеспечивает минимальные суммарные затраты на систему защиты информации и потери от остающихся потенциальных угроз после внедрения системы защиты информации. В статье представлена новая робастная схема, обеспечивающая устойчивое решение поставленной задачи оптимизации затрат на систему защиты информации в условиях неопределенности величин потерь от хакерских атак. Схема основана на робастном методе сглаживания и итерационной схеме нахождения слаженной компоненты, в которой для построения целевой функции оптимизационной задачи используется робастная функция Тьюки. Представленная робастная схема позволяет находить устойчивое решение задачи минимизации материальных затрат в том числе в условиях аномальных выбросов уровней хакерских атак.

Ключевые слова: системы управления, сетевые каналы связи, хакерские атаки, защита информации, математическая модель затрат на систему защиты, оптимизация затрат на защиту информации

DOI: 10.1134/S2304487X21030068

ВВЕДЕНИЕ

Защита конфиденциальной информации предприятий электронной промышленности и всей отрасли в целом, прежде всего баз данных, помещаемых в системах с потенциальной угрозой взлома систем защиты и получения доступа к защищаемой информации, требует существенных затрат. Поэтому необходимо решить задачи минимизации этих затрат при условии обеспечения необходимого уровня защиты охраняемой информации от внешних угроз. Поскольку потери от угроз носят неопределенный характер, в настоящей работе они трактуются как случайные величины и можно использовать различные постановки задачи оптимизации при установлении системы защиты от угроз [1–6].

1. СХЕМА ОПТИМИЗАЦИИ ЗАТРАТ НА СИСТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УГРОЗ

В работе [7] задача оптимизации затрат на систему защиты информации ставится как задача, основанная на минимизации суммарных затрат на реализацию системы защиты и средних потерь из-за угроз, которые могут реализоваться после установления системы защиты, а для определения средних потерь используется робастная схема Хьюбера.

В настоящей работе для определения средних потерь используется новая робастная схема, позволяющая получать более устойчивые оценки средних значений потерь в условиях наличия аномальных выбросов потерь.

Целевая функция задачи оптимизации затрат на систему защиты информации имеет следующий вид

$$\psi(L) = L + MP(L), \qquad (1)$$

где L – затраты на систему защиты, $MP(L)$ – среднее значение потерь $P(L)$ от угроз с системой защиты, затраты на реализацию которой составили L.

Статистика значений случайных величин (случайной функции) $P(L)$ может быть получена в

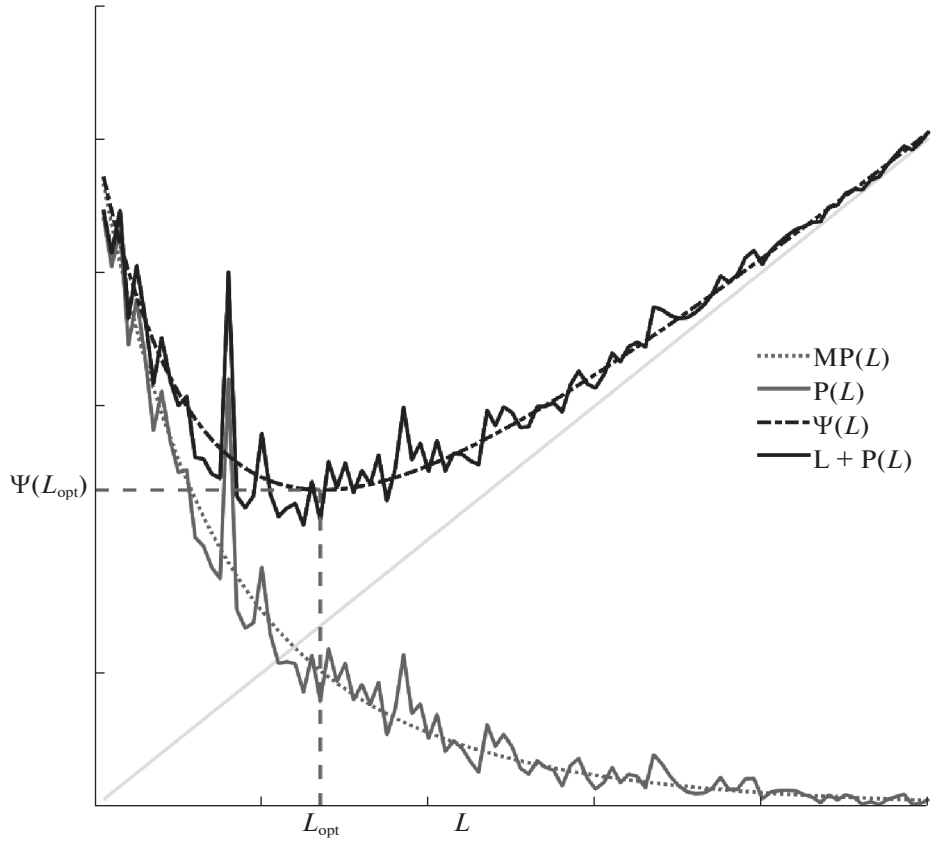

Рис. 1. Затраты на систему защиты информации и потери от реализованных угроз. Тестовый пример 1.

процессе опытных поэтапных испытаний систем защиты при разных значениях величины затрат на систему защиты PL, либо на основе теоретической модели угроз и их дальнейшего воспроизводства для расчетного базового периода с помощью схемы статистических испытаний Монте-Карло.

Функцию $MP(L)$ можно получить с помощью методов сглаживания и основанных на них схем и алгоритмов. Для получения $MP(L)$ необходимо использовать робастные методы сглаживания (выделения детерминированной компоненты исходной случайной функции $P(L)$) поскольку угрозы могут носить аномальный характер по величине возможных потерь.

Ниже приведена новая используемая в работе схема робастного сглаживания и основанный на ней алгоритм, реализованный в компьютерной программе для расчета оптимальной величины затрат на систему защиты.

Пусть известны реализованные значения потерь $P(L)_i = L_i$, $i = 1,\ldots,n$ при затратах на систему защиты $L_i, i = 1,\ldots,n$ соответственно.

Тогда сглаженную детерминированную компоненту $MP_{sm}(L)$ случайной функции $P(L)$ можно представить в виде разложения [8]:

$$MP_{sm}(L) = \sum_{j=1}^{m} u_j \cdot \Phi_j(L), \qquad (2)$$

где $\Phi_j(x)$ – базисная система линейно независимых функций.

Коэффициенты $u_j, j = 1,\ldots,m$ представления (2) определяются с помощью итерационного процесса:

$$\vec{u}^{(k+1)} = (A_k^T \cdot A_k)^{-1} \cdot A_k^T \cdot \vec{f}^{(k)}, \quad k = 0,1,\ldots \qquad (3)$$

где k – номер итерации, элементы a_{ij}, $i = 1, \ldots, n_k$, $n_0 = n, j = 1,\ldots,m$ матрицы A_k определяются равенствами:

$$a_{kij} = \Phi_j(L_i), \quad i = i_1,\ldots,i_{n_k}, \quad j = 1,\ldots,m, \qquad (4)$$

а компоненты векторов $\vec{f}^{(k)}$, $k = 0,1,\ldots$ равенствами:

$$\vec{f}^{(0)} = (L_1,\ldots,L_n)^T,$$
$$\vec{f}^{(k)} = (f_1^{(k)},\ldots,f_{n_k}^{(k)})^T, \quad k = 1,\ldots \qquad (5)$$

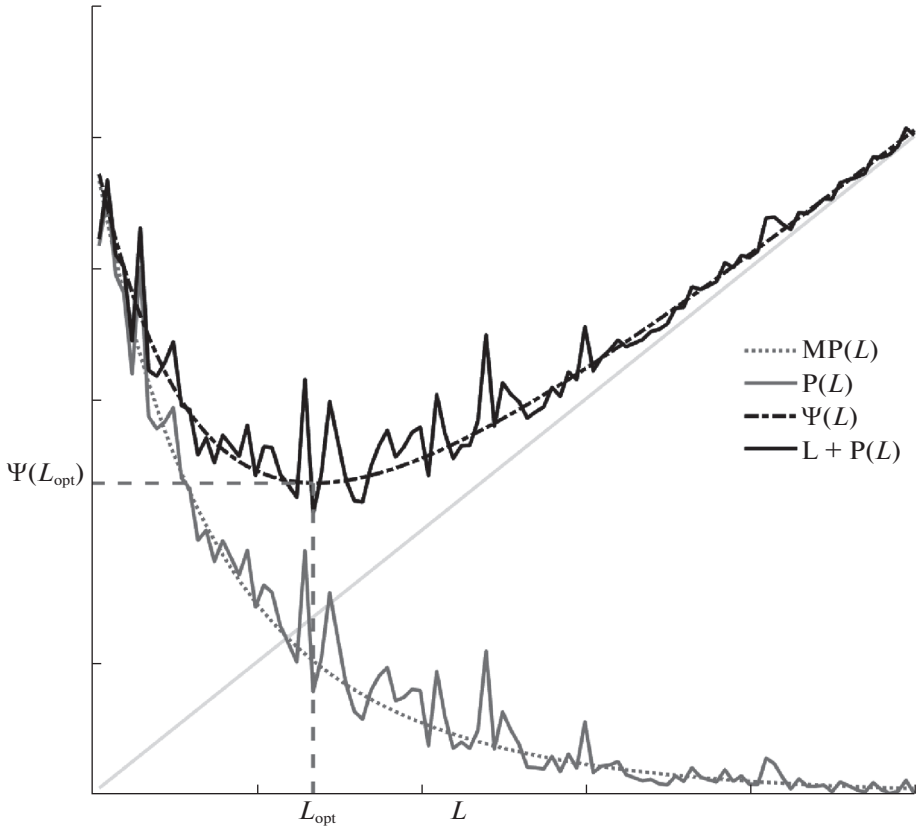

Рис. 2. Затраты на систему защиты информации и потери от реализованных угроз. Тестовый пример 2.

$$f_i^{(k)} = L_i, \quad \text{если} \quad i \in I_0^{(k)}, \tag{6}$$

где индексам $i = i_1,\ldots,i_{n_k}$ соответствуют выполнению неравенств

$$I_0^{(k)} = \left\{ i : \left| P(L_{i_k}) - \sum_{j=1}^{m} u_j^{(k)} \cdot \Phi_j(L_i) \right| \le H \cdot \sigma^{(k)} \right\}, \tag{7}$$

$$\sigma^{(k)2} = \frac{1}{n_k} \cdot \sum_{i_k} \left(P(L_{i_k}) - \sum_{j=1}^{m} u_j^{(k)} \cdot \Phi_j(L_{i_k}) \right)^2, \tag{8}$$

а отсутствующим индексам i неравенства $\left| P(L_{i_k}) - \sum_{j=1}^{m} u_j^{(k)} \cdot \Phi_j(L_i) \right| > H \cdot \sigma^{(k)}$.

В общем случае оптимальное значение параметра $H = 1.8$ (см. [8]).

Итерационный процесс (3)–(8) сходится за конечное число итераций [8].

2. ЧИСЛЕННЫЕ РЕЗУЛЬТАТЫ

На рис. 1, 2 представлены тестовые исходные данные и результаты их обработки в процессе решения задачи оптимизации затрат на систему защиты информации. Тестовые исходные данные по потерям из-за угроз были получены с помощью датчика χ^2 – распределенной случайной величины и с учетом монотонного убывания функции $ML(PL)$ при увеличении затрат на систему защиты.

Графики функций $\psi(L)$ и $MP(L)$ на рисунках 1, 2 обозначены пунктирными линиями. На рисунках 1, 2 выделено оптимальное значение затрат L_{opt}, при котором достигается минимальное значение целевой функции $\psi(L)$.

ЗАКЛЮЧЕНИЕ

Следует отметить, что не для любой системы защиты информации от угроз существует минимум целевой функции $\psi(L)$ при положительном значении затрат L.

Действительно, если, при условии монотонного убывания функции $MP(L)$, производная $\frac{dMP(L)}{dL}$ удовлетворяет неравенству $\frac{dMP(L)}{dL} > -1$, то целевая функция $\psi(L)$ – монотонно возрастающая и, тем самым, аппаратура такой системы защиты

информации не эффективна и не может использоваться для защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. *Тараторин Д.И.* Анализ угроз информационной безопасности на предприятиях распределенного типа // Проектирование информационных систем. СПб.: СПбГИЭУ, 2006.
2. *Середа С.А.* Анализ средств преодоления систем защиты программного обеспечения // ИНФОРМОСТ: Радиоэлектроника и телекоммуникации. 2002. № 4 (22).
3. *Баутов А.* Стандарты и оценка эффективности защиты информации // Доклад на Третьей всероссийской практической конференции “Стандарты в проектах современных информационных систем”. Москва, 23–24 апреля 2003.
4. *Козлов В.* Критерии информационной безопасности и поддерживающие их стандарты: состояние и тенденции. “Стандарты в проектах современных информационных систем” // Сб. трудов II-й всероссийской практической конференции. Москва, 27–28 марта 2002.
5. *Кияев В.И., Граничин О.Н.* Безопасность информационных систем. М.: Открытый Университет “ИНТУИТ”, 2016, 192 с.
6. *Родионов А.С., Белянин В.И., Горбунов А.А.* Совершенствование методов защиты информации от несанкционированного доступа // NBI Technologies. 2018. V. 12. № 2.
7. *Kryanev A.V., Kudryashov N.A., Sliva D.E.* Cost optimization for information security systems // Journal of Physics: Conference Series. 1686 (2020) 012033.
8. *Крянев А.В., Лукин Г.В., Удумян Д.К.* Метрический анализ и обработка данных. М.: Физматлит, 2012.

Vestnik Natsional’nogo issledovatel’skogo yadernogo universiteta “MIFI”, 2021, vol. 10, no. 3, pp. 239–243

Mathematical Model of Optimizing Expenditure on the Information Protection System in the Network Communication Channels of Control Systems

S. G. Klimanov[a], A. V. Kryanev[a,#], and N. A. Kudryashov[a]

[a] *National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, 115409 Russia*

[#] *e-mail: AVKryanev@mephi.ru*

Received July 6, 2021; revised July 7, 2021; accepted July 13, 2021

Abstract—The urgent problem of protecting information that may become available through network communication channels from hacker attacks is considered. This task is associated with the storage and transmission of information in the management systems of individual enterprises and industries, in particular the electronics industry. To create a system for protecting information from threats, material costs are required, the value of which increases with the level of information protection. A mathematical scheme is proposed to determine such an optimal level of material costs in the information protection system, which ensures the minimum total costs for the information protection system and losses from remaining potential threats after the information protection system is implemented. A new robust scheme is presented to provide a stable solution to the problem of optimizing the cost of an information security system under conditions of uncertainty in the values of losses from hacker attacks. The scheme is based on a robust smoothing method and an iterative scheme for finding a harmonized component, in which the Tukey robust function is used to construct the objective function of the optimization problem. The presented robust scheme makes it possible to find a stable solution to the problem of minimizing material costs, including in conditions of abnormal emissions of the levels of hacker attacks.

Keywords: control systems, network communication channels, hacker attacks, information protection, mathematical model of costs for a protection system, optimization of costs for information protection

DOI: 10.1134/S2304487X21030068

REFERENCES

1. Taratorin D.I. Analiz ugroz informatsionnoi bezopasnosti na predpriyatiyah raspredelennogo tipa [Analysis of information security threats in distributed enterprises].*Proektirovanie informatsionnih sistem*. SPb.: SPbGIEU, 2006. (in Russian)
2. Sereda S.A. Analiz sredstv preodoleniya system zashiti programmnogo obespecheniya.[Analysis of means of overcoming software protection systems]. *INFORMOST: Radioelektonika i Telecommunicatsii*, 2002. no. 4 (22). (in Russian)
3. Bautov A. [Standarti i otsenka effektivnosti zashiti informatsii]. *Doklad na Tretei Vserossiiskoi prakticheskoi*

konferencii "Standarti v proektah sovremennih informtsionnih system. [Report at the Third All-Russian Practical Conference "Standards in projects of modern information systems"]. Moscow, 2003. (in Russian)

4. Kozlov V. [Kriterii informatsionnoi bezopasnosti i poddergivaushie ih standarti sostoyaniya i tendentsii. "Standarti v proektah sovremennih informatsionnih system"]. *Sbornik trudov 2-i Vserossiskoi paktichеskoi konferentsii*. [Proceedings of the 2-th All-Russian Practical Conference], Moscow, 2002. (in Russian)
5. Kiyaev V.I., Granichin O.N. *Bezopasnost informatsionnih system*. [Security of information systems]. Moscow. Otkritii unuversitet "INTUIT" Publ, 2016. 192 p.
6. Rodionov A.S., Belyanin V.I., Gorbunov A.A. Sovershenstvovanie metodov zashiti informatsii ot nesankcionirovannogo dostupa. [Improving the methods of protecting information from unauthorized access]. *NBI Technologies*. 2018, vol. 12, no. 2.
7. Kryanev A.V., Kudryashov N.A. and Sliva D.E. Cost optimization for information security systems. Journal of Physics: Conference Series, 2020. 1686.
8. Kryanev A.V., Lukin G.V., Udumyan D.K. *Metricheskii analiz i obrabotka dannih* [Metric analysis and data processing]. Moscow, Fizmatlit Publ., 2012.