

УДК 616.718.4-001.5-08

https://doi.org/10.33619/2414-2948/85/45

АНАЛИЗ МЕТОДОВ И МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

©*Калмуратова С. М., Каракалпакский государственный университет им. Бердаха, г. Нукус, Узбекистан*

©*Нукусбаев Н. Ж., Каракалпакский государственный университет им. Бердаха, г. Нукус, Узбекистан, nawriznukusbaev@karsu.uz*

ANALYSIS OF METHODS AND METHODOLOGY FOR ASSESSING THE EFFICIENCY OF INFORMATION PROTECTION SYSTEMS

©*Kalmuratova S., Karakalpak State University named after Berdakh, Nukus, Uzbekistan,*

©*Nukusbaev N., Karakalpak State University named after Berdakh, Nukus, Uzbekistan, nawriznukusbaev@karsu.uz*

Аннотация. Представлены основные методы оценки эффективности систем защиты информации информационных систем, их преимущества и недостатки. Существуют недостатки оценки эффективности СЗИ, связанные с выбором показателей, сложная вычислительная нагрузка, недостатки экспертных оценок и необходимость привлечения высококвалифицированных специалистов.

Abstract. Presents the main methods for evaluating the effectiveness of information security systems of information systems, their advantages and disadvantages. There are shortcomings in evaluating the effectiveness of the information security system associated with the choice of indicators, a complex computational load, shortcomings in expert assessments and the need to attract highly qualified specialists.

Ключевые слова: вероятность, система, метод минимизации, системы защиты информации.

Keywords: probability, system, minimization method, Information Security Systems.

Основными методами оценки эффективности системы защиты информации информационных систем являются: статистический; вероятностный; частотный; экспертный; информационно-энтропийный; многокритериальный (нейросетевой); метод минимизации рисков; матричный (формальный); многоуровневый; комбинаторный (оптимизационный).

Метод минимизации рисков. Реализуется следующими шагами: 1. Фиксация рисков. 2. Индекс риска. 3. Проводится классификация рисков. 4. Определяются способы обработки рисков. 5. Рассчитываются показатели, характеризующие риски. 6. Рассчитываются показатели экономического эффекта от управления рисками [1].

Одновременно с этим существуют ряд проблем, связанных с выбором показателей оценки эффективности СЗИ [2, 3].

Анализ методов и методик оценки эффективности СЗИ показал, что в настоящее время существуют недостатки оценки эффективности СЗИ, связанные с выбором показателей, сложная вычислительная нагрузка, недостатки экспертных оценок и необходимость привлечения высококвалифицированных специалистов в области ИБ.

Таблица

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ МЕТОДОВ
 ОЦЕНКИ ЭФФЕКТИВНОСТИ СЗИ (СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ)

Метод оценки СЗИ ИС	Преимущества	Недостатки
Статистический	Позволяет получать результаты в случаях, когда не известны параметры СЗИ (систем защиты информации) и СФ (среда функционирования), позволяет оценивать СЗИ ТРИС (территориально-распределенных ИС) любой сложности	Результаты достоверны с определенной вероятностью, большой объем обработки статистических данных
Вероятностный	Анализируется полный спектр УБИ, использование реалистичного подхода, взаимосвязи между элементами СЗИ ТРИС (территориально-распределенных ИС) учитываются в явном виде	Сложность вычислений, невозможно обнаружить плавное изменение вероятностных характеристик наблюдений
Частотный	Удобство реализации, графическое представление характеристик СЗИ ТРИС	Необходимость в большой статистической выборке
Экспертный	Использование метода в отсутствии статистических сведений. Быстрота получения результатов.	Человеческий фактор — достоверность результатов зависит от компетенций экспертов. Субъективность метода. Потребность в высококвалифицированных специалистах по ИБ. Недостаточная устойчивость
Информационно-энтропийный	По характеру зависимости $\Psi(t)$ удобно судить об эффективности СЗИ ТРИС. Если вид зависимости отличается от линейной, то можно сделать вывод о неэффективности СЗИ ИБ (информационной безопасности)	Необходимость принятия пороговых значений для оценивания результатов вычислений или составление эталонных образцов, что вызывает трудности в связи с ограниченностью и неполнотой результатов эксперимента. Не рассматривается стохастическая природа событий и явлений, которые возникают в процессе обеспечения ИБ
Многокритериальный (нейро сетевой)	Позволяет учитывать большое количество критериев оценки СЗИ ТРИС. Позволяет учитывать не только количественные, но и качественные показатели критериев оценки СЗИ ТРИС. Позволяет преодолевать неопределенности	Сложность выбора оптимальной структуры. Отсутствие формализованных процедур выбора измеряемых параметров (показатели оценки СЗИ ТРИС). Требуется больших вычислительных ресурсов
Метод минимизации рисков	Отсутствие необходимости в точной и полной информации. Простота в части использования инструментальных средств проведения оценки эффективности СЗИ ТРИС	Сложность при проведении оценки рисков. Результат зависит от экспертной оценки рисков. Использование нескольких оптимизационных моделей
Матричный (формальный)	Универсальный метод для проведения оперативной. Оценки эффективности СЗИ ТРИС. Требуется минимальных вычислительных ресурсов	Не позволяет проводить оценку эффективности СЗИ ТРИС в условиях неопределенности, большого числа показателей оценки
Многоуровневый	Повышение объективности и корректности оценки эффективности	Сложность формирования уровней оценивания СЗИ ТРИС. Сложность

Метод оценки СЗИ ИС	Преимущества	Недостатки
	СЗИ ТРИС, позволяет обрабатывать трудно формализуемые данные качественных характеристик и нечеткой информации	проведения вычислений
Комбинаторный (оптимизационный)	Наиболее эффективный методом в оценке эффективности СЗИ ТРИС. Гибкость построения	Сложность поведения вычислений

Под оценкой эффективности понимается следующее: эффективность СЗИ достигается путем создания СЗИ, способной максимально нейтрализовать актуальные УБИ в ТРИС, выполнить требования по защите информации, предъявляемые к ТРИС на основании требований регуляторов в области обеспечения безопасности информации, а также позволяющей снизить финансовые затраты на создание СЗИ.

Список литературы:

1. Гвоздик Я. М. Модель и методика оценки систем защиты информации автоматизированных систем: дисс. ... канд. техн. наук. СПб. 2011.
2. Коломойцев В. С. Модели и методы оценки эффективности систем защиты информации и обоснование выбора их комплектации: дисс. ... канд. техн. наук. СПб. 2018.
3. Миняев А. А. Метод и методика оценки эффективности системы защиты территориально-распределенных информационных систем // Информатизация и связь. 2020. №6. С. 29-36.

References:

1. Gvozdik, Ya. M. (2011). Model' i metodika otsenki sistem zashchity informatsii avtomatizirovannykh sistem: diss. ... kand. tekhn. nauk. St. Petersburg. (in Russian).
2. Kolomoitsev, V. S. (2018). Modeli i metody otsenki effektivnosti sistem zashchity informatsii i obosnovanie vybora ikh komplektatsii: diss. ... kand. tekhn. nauk. St. Petersburg. (in Russian).
3. Minyaev, A. A. (2020). Metod i metodika otsenki effektivnosti sistemy zashchity territorial'no-raspredeleennykh informatsionnykh system. *Informatizatsiya i svyaz'*, (6), 29-36. (in Russian).

*Работа поступила
в редакцию 10.11.2022 г.*

*Принята к публикации
19.11.2022 г.*

Ссылка для цитирования:

Калмуратова С. М., Нукусбаев Н. Ж. Анализ методов и методика оценки эффективности систем защиты информации // Бюллетень науки и практики. 2022. Т. 8. №12. С. 382-384. <https://doi.org/10.33619/2414-2948/85/45>

Cite as (APA):

Kalmuratova, S., & Nukusbaev, N. (2022). Analysis of Methods and Methodology for Assessing the Efficiency of Information Protection Systems. *Bulletin of Science and Practice*, 8(12), 382-384. (in Russian). <https://doi.org/10.33619/2414-2948/85/45>