Scientific and Practical Cyber Security Journal (SPCSJ) 6(1): 64-71 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

ПОКАЗАТЕЛИ И МАТЕМАТИЧЕСКИЕ КРИТЕРИИ ОЦЕНИВАНИЯ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И КИБЕРБЕЗОПАСНОСТИ ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

INDICATORS AND MATHEMATICAL CRITERIA FOR EVALUATING THE EFFECTIVENESS OF THE INFORMATION SECURITY SYSTEM AND CYBERSECURITY OF THE OBJECT OF CRITICAL INFORMATION INFRASTRUCTURE

к.т.н., Козубцова Леся Михайловна,Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Candidate of Engineering Sciences, Lesya Kozbtsova,Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
к.т.н., Гуда Оксана Викторовна,Луцкий национальный технический университет, г. Луцк, Украина
Candidate of Technical Sciences, Oksana, Guda Lutsk National Technical University, Lutsk, Ukraine
к.т.н., Крадинова Татьяна Адамовна,Луцкий национальный технический университет, г. Луцк, Украина
Candidate of Technical Sciences, Tatyana Kradinova, Lutsk National Technical University, Lutsk, Ukraine
Палагута Анастасия Михайловна Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Palaguta Anastasia Military Institute of Telecommunications and Informatization named after Heroes of Krut, Kiev, Ukraine
д.п.н., к.т.н., профессор РАЕ Козубцов Игорь Николаевич, Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Doctor of Pedagogical Sciences, Candidate of Engineering Sciences, Professor of RAE, Igor Kozubtsov, Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine

АННОТАЦИЯ. Каждого руководителя (распорядителя) объекта критической информационной инфраструктуры интересует ответ на вопрос как оценить эффективность функционирования систему защиты информации и кибербезопасности. Актуальность темы исследований обусловлено отсутствием показателей и математических критериев оценивания эффективности функционирования объектов критической информационной инфраструктуры. **Основные аспекты работы.** Для однозначного ответа на вопрос, как и чем оценить эффективность функционирования системы защиты информации и кибербезопасности в статье продолжены показатели и математические критерии эффективности. **Научная новизна.** Научная новизна полученного результата заключается в том, что предложены показатели и определены математические критерии возможной оценки эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры.

КЛЮЧЕВЫЕ СЛОВА: *показатель, критерий эффективности, функционирование, система, защита информации, кибербезопасность, объект критической информационной инфраструктуры.*

ABSTRACT. Each manager (manager) of a critical information infrastructure facility is interested in the answer to the question of how to evaluate the effectiveness of the information security and cybersecurity system. The relevance of the research topic is due to the lack of indicators and mathematical criteria for evaluating the effectiveness of the functioning of critical information infrastructure facilities. The main aspects of the work. For an unambiguous answer to the question of how and how to evaluate the effectiveness of the functioning of the information security and

cybersecurity system, the article considers the indicators and mathematical criteria of effectiveness. Scientific novelty. The scientific novelty of the obtained result lies in the fact that indicators are proposed and mathematical criteria for possible evaluation of the effectiveness of the information security system and cybersecurity of critical information infrastructure objects are determined.

KEYWORDS: *indicator, efficiency criterion, functioning, system, information protection, cybersecurity, object of critical information infrastructure.*

ВВЕДЕНИЕ

Система защиты информации и кибербезопасности (СЗИКБ) – это сложный комплекс программных, криптографических, организационных и других средств, методов и мероприятий, предназначенных для защиты информации и кибербезопасности. Так как система «Система защиты информации и кибербезопасности» является относительно новой, то для нее еще неразработанное метрологическое обеспечения. Тем не менее каждого руководителя объекта критической информационной инфраструктуры (ОКИИ) интересует ответа на вопрос, в какой степени его настроенная система защиты информации и кибербезопасности ОКИИ обеспечивает необходимый уровень кибербезопасности. Ответом на этот вопрос может служить результат оценивания эффективности системы защиты информации и кибербезопасности по частичным показателям, которые носят вероятностный характер. Эффективность системы – это свойство системы, характеризующее ее способность выполнять свою целевую функцию в заданиях условиях. То есть под эффективностью системы понимают степень достижения цели этой системой. Тогда применительно к нашей системы под эффективностью системы защиты информации и кибербезопасности ($E_{СЗИКБ}$) будем понимать степень соответствия достигнутых результатов поставленным целям по защите информации.

Для осуществления оценки эффективности функциональной способности системы защиты информации и кибербезопасности ОКИИ необходимо наличие методики проведения, совокупность показателей оценивания и критерий оценки – признаков, основание принятия решения относительно оценки эффективности на соответствие предъявленным требованиям.

В связи с отсутствием для нового объекта исследования показателей и критерий оценивания в данном исследовании возникает необходимость в решении новой научной задачи. Сформулируем ее в следующей постановке. Необходимо изучить подходы и показатели, их математические модели, позволяющие оценить эффективности функционирования системы защиты информации и кибербезопасности.

АНАЛИЗ ПОСЛЕДНИХ ИССЛЕДОВАНИЙ И ПУБЛИКАЦИЙ ПО ДАННОМУ НАПРАВЛЕНИЮ

Анализ последних исследований и публикаций для целостности проведем в основной части нашего исследования.

Решение вопроса по выбору критериев оценки эффективности функционирования любой системы защиты по показателю максимального эффекта предложено в работе [1]. Расчет осуществляется по формуле (1):

$$E = Эф/В \quad (1)$$

где Е – под эффективностью понимают степень достижения цели этой системой;

Эф – эффект, который достигается при внедрении данной системы;

В – расходы, совокупные расходы на приобретение, установку и конфигурирование, сопровождение и поддержку, а также затраты связанные с простоем оборудования вовремя техническое обслуживание или устранение неисправностей системы.

Однако ввиду специфики использования СЗИКБ определить прямой эффект от их внедрения (в временных или финансовых этого возникает задача выбора метода оценки, все множество показателях) трудно. Применение данного подхода требует наличия методики расчета стоимости потери информационных активов, без которых невозможно осуществлять расчет эффективности функционирования системы защиты информации и кибербезопасности.

Подход к оценке эффективности функционирования системы защиты информации и кибербезопасности в информационно-телекоммуникационных системах по показателю предотвращения потерь. Расходы на обеспечение информационной безопасности следует считать эффективными, если они обеспечивают выполнение требований нормативных документов и стандартов, принятых государством, а также концепции информационной

безопасности организации.

Предложенный метод оценки экономической эффективности подразделения по защите информации [2] не совсем решает поставленную задачу. Для расчета показателя эффективности по результату внедрения и проведения мероприятий по обеспечению информационной и кибербезопасности необходимо иметь значение предотвращенных потерь (ЗВ). Он рассчитываются исходя из вероятности возникновения инцидента информационной и кибербезопасности и возможных экономических потерь от него до и после реализации мероприятий по обеспечению кибербезопасности. Применение данного подхода затруднено вследствие отсутствия подходов к расчету В1 и В2.

Изложенный в работе [3] подход к оценке эффективности мероприятий информационной безопасности в условиях неопределенности позволяет продолжить поиск в этом направлении и предложить еще другие показатели, которые могут охарактеризовать эффективности функциональной способности системы защиты информации и кибербезопасности ОКИИ.

ЦЕЛЬ СТАТЬИ

Рассмотреть показатели и критерии оценивания эффективности функционирования системы защиты информации и кибербезопасности ОКИИ.

ОСНОВНОЙ РЕЗУЛЬТАТ ИССЛЕДОВАНИЯ

Прежде чем выбрать возможные показатели и математические критерии оценивания эффективности функционирования системы защиты информации и кибербезопасности объекта критической информационной инфраструктуры, рассмотрим некоторые определения.

Средство криптографической защиты информации – программный, аппаратно-программный и аппаратный средство, предназначенное для криптографической защиты информации.

Средства технической защиты информации – программный, аппаратно-программный и аппаратный инструмент, предназначенный для технической защиты информации и имеет соответствующее экспертное заключение.

Средство кибернетической защиты информации – программный, аппаратно-программный и аппаратный средство, предназначенное для киберзащиты информации.

Показатель эффективности – это величина, характеризующая степень достижения системой любой из поставленных перед ней задач.

Требования к показателю эффективности: иметь определенный физический смысл; быть пригодным для количественного анализа; иметь простую и удобную форму; отражать одну из значимых сторон функционирования системы; обеспечивать необходимую чувствительность.

Единичные (частные) показатели эффективности, отражают какую-то из значимых сторон функционирования системы (вероятность обнаружения нарушителя или вероятность его нейтрализации силами охраны и т.п.);

Комплексные (обобщенные) показатели эффективности, представляют собой комбинацию частичных показателей.

Согласно этого определения предложим следующие частные показатели эффективности, как числовые величины, которые будут характеризовать степень достижения системой защиты информации и кибербезопасности поставленных перед ней задач:

киберзащищенность ($P_{КЗ}$). Киберзащищенность – способность системы связи выполнять задачи по назначению в условиях программно-математических воздействий противника, то есть вероятность того, что эта система будет защищенной от кибернетического вмешательства;

коэффициент укомплектованности средствами криптографической защиты информации, технической защиты информации и киберзащиты ($K_{УС}$). Показатель укомплектованность средствами криптографической защиты информации, технической защиты информации и киберзащиты характеризуется соотношением штатных и в наличии средств криптографической защиты информации, технической защиты информации и киберзащиты. Показатель рассчитывается отдельно по средствам криптографической защиты информации, технической защиты информации и киберзащиты;

коэффициент технической готовности средств криптографической защиты информации, технической защиты информации и киберзащиты ($K_{ТГС}$). Коэффициент технической готовности – отношение количества технически исправных средств криптографической защиты информации, технической защиты информации и киберзащиты к фактически имеющаяся в

наличии. Характеризует готовность средств к применению по назначению и показывает, насколько хорошо поддерживается техническое состояние средств криптографической защиты информации, технической защиты информации и киберзащиты на ОКИИ.

коэффициент укомплектованности исправными средствами криптографической защиты информации, технической защиты информации и киберзащиты ($К_{УИС}$). Коэффициент технической готовности – отношение количества технически исправных средств криптографической защиты информации, технической защиты информации и киберзащиты к их списочному количеству. Характеризует готовность средств к применению по назначению и показывает, насколько хорошо поддерживается техническое состояние средств криптографической защиты информации, технической защиты информации и киберзащиты на ОКИИ;

коэффициент укомплектованности штатных должностей системными администраторами ($К_{СА}$). Показатель укомплектованность штатных должностей системными администраторами характеризуется соотношением штатных и к занятым должностям;

коэффициент укомплектованности штатных должностей обслуживающим персоналом ($К_{СА}$). Показатель укомплектованность штатных должностей обслуживающим персоналом характеризуется соотношением штатных и к занятым должностям;

киберзащищенность по результатам penetration testing($P_{КЗ}^{РТ}(S)$). Реальное значение киберзащищенность ОКИИ по результатам активного тестирования.

Математическая модель расчета эффективности функционирования системы защиты информации и кибербезопасности в ОКИИ по показателю киберзащищённости. Под киберзащищённостью будем понимать способность системы выполнять задачи по назначению в условиях программно-математических воздействий [1].

Для реализации на практике оценивания эффективности функционирования системы защиты информации и кибербезопасности ОКИИ по показателю киберзащищённости рекомендуется применить методику, изложенную в работе [4; 5] адаптировав ее для решения новой задачи.

Киберзащищенность в первом приближении может служить ярким индикатором эффективности функционирования системы защиты информации и кибербезопасности ОКИИ (2):

$$E_{СЗIКБ} \approx P_{КЗ} \quad (2)$$

Расчет коэффициента укомплектованности средствами криптографической защиты информации, технической защиты информации и киберзащиты предлагается осуществляется по формуле (3):

$$К_{УС} = \frac{Ф_С}{Ш_С} \quad (3)$$

где $К_{УС}$ – коэффициент укомплектованности средствами криптографической защиты информации, технической защиты информации и киберзащиты;

$Ш_С$ – штатная численность средств криптографической защиты информации, технической защиты информации и киберзащиты;

$Ф_С$ – фактически имеющаяся численность средств криптографической защиты информации, технической защиты информации и киберзащиты;

Оценивания способности укомплектованности средствами системы защиты информации и кибербезопасности в ОКИИ критически оказывать влияние на $Э_{СЗИКБ}$ предлагается осуществлять по критериям наведённых в табл. 1.

Таблица 1. *Критерии оценивания способности укомплектованности средствами системы защиты информации и кибербезопасности в ОКИИ критически оказывать влияние на $Э_{СЗИКБ}$*

Критерий эффективности $Э_{СЗИКБ}$	коэффициент укомплектованности средствами				
	$0 \le К_{УС} \le 0{,}25$	$0{,}25 < К_{УС} \le 0{,}5$	$0{,}5 < К_{УС} \le 0{,}75$	$0{,}75 < К_{УС} \le 0{,}9$	$0{,}9 < К_{УС} \le 1$
	Очень низкий (ОН)	Низкий (Н)	Средний (С)	Высокий (В)	Очень высокий (ОВ)
$0 \le Э_{СЗИКБ} \le 0{,}25$	ОН	ОН	ОН	ОН	ОН
$0{,}25 < Э_{СЗИКБ} \le 0{,}5$	Н	Н	Н	Н	Н
$0{,}5 < Э_{СЗИКБ} \le 0{,}75$	С	С	С	С	С
$0{,}75 < Э_{СЗИКБ} \le 0{,}9$	С	С	С	В	В
$0{,}9 < Э_{СЗИКБ} \le 1$	В	В	В	В	ОВ

Расчет технической готовности средств криптографической защиты информации, технической защиты информации и киберзащиты осуществляется по формуле (4):

$$К_{ТГС} = \frac{Ф_{ИС}}{Ф_{С}}. \quad (4)$$

где $К_{ТГС}$ – коэффициента технической готовности средств криптографической защиты информации, технической защиты информации и киберзащиты;

$Ф_{ИС}$ – количество исправных средств криптографической защиты информации, технической защиты информации и киберзащиты;

$Ф_{С}$ – фактически имеющаяся численность средств криптографической защиты информации, технической защиты информации и киберзащиты;

Оценивания способности технической готовности средствами системы защиты информации и кибербезопасности в ОКИИ критически оказывать влияние на $Э_{СЗИКБ}$ предлагается осуществлять по критериям наведённых в табл. 2.

Таблица 2. *Критерии оценивания технической готовности средствами системы защиты информации и кибербезопасности в ОКИИ критически оказывать влияние на $Э_{СЗИКБ}$*

Критерий эффективности $Э_{СЗИКБ}$	коэффициент технической готовности средств				
	$0 \le K_{ТГС} \le 0,25$	$0,25 < K_{ТГС} \le 0,5$	$0,5 < K_{ТГС} \le 0,75$	$0,75 < K_{ТГС} \le 0,9$	$0,9 < K_{ТГС} \le 1$
	Очень низкий (ОН)	Низкий (Н)	Средний (С)	Высокий (В)	Очень высокий (ОВ)
$0 \le Э_{СЗИКБ} \le 0,25$	ОН	ОН	ОН	ОН	ОН
$0,25 < Э_{СЗИКБ} \le 0,5$	Н	Н	Н	Н	Н
$0,5 < Э_{СЗИКБ} \le 0,75$	С	С	С	С	С
$0,75 < Э_{СЗИКБ} \le 0,9$	С	С	С	В	В
$0,9 < Э_{СЗИКБ} \le 1$	В	В	В	В	ОВ

Расчет коэффициента укомплектованности исправными средствами криптографической защиты информации, технической защиты информации и киберзащиты осуществляется по формуле (5):

$$К_{УИС} = К_{УС} \times К_{ТГС} = \frac{Ф_{ИС}}{Ш_{С}} \quad (5)$$

где $К_{УИС}$ – коэффициента укомплектованности исправными средствами криптографической защиты информации, технической защиты информации и киберзащиты;

$К_{УС}$ – коэффициента укомплектованности средств криптографической защиты информации, технической защиты информации и киберзащиты;

$К_{ТГС}$ – коэффициента технической готовности средств криптографической защиты информации, технической защиты информации и киберзащиты;

$Ф_{ИС}$ – количество исправных средств криптографической защиты информации, технической защиты информации и киберзащиты;

$Ш_{С}$ – штатная численность средств криптографической защиты информации, технической защиты информации и киберзащиты.

Оценивания способности укомплектованности исправными средствами системы защиты информации и кибербезопасности в ОКИИ критически оказывать влияние на $Э_{СЗИКБ}$ предлагается осуществлять по критериям наведённых в табл. 3.

Таблица 3. *Критерии оценивания укомплектованности исправными средствами системы защиты информации и кибербезопасности в ОКИИ критически оказывать влияние на $Э_{СЗИКБ}$*

Критерий эффективности $Э_{СЗИКБ}$	коэффициент укомплектованности исправными средствами				
	$0 \le K_{УИС} \le 0,25$	$0,25 < K_{УИС} \le 0,5$	$0,5 < K_{УИС} \le 0,75$	$0,75 < K_{УИС} \le 0,9$	$0,9 < K_{УИС} \le 1$
	Очень низкий (ОН)	Низкий (Н)	Средний (С)	Высокий (В)	Очень высокий (ОВ)
$0 \le Э_{СЗИКБ} \le 0,25$	ОН	ОН	ОН	ОН	ОН
$0,25 < Э_{СЗИКБ} \le 0,5$	Н	Н	Н	Н	Н
$0,5 < Э_{СЗИКБ} \le 0,75$	С	С	С	С	С
$0,75 < Э_{СЗИКБ} \le 0,9$	С	С	С	В	В
$0,9 < Э_{СЗИКБ} \le 1$	В	В	В	В	ОВ

Расчет коэффициента укомплектованности штатных должностей системными администраторами системы защиты информации и кибербезопасности ОКИИ осуществляется по формуле (6):

$$К_{СА} = \frac{Ф_{СА}}{Ш_{СА}} \quad (6)$$

где $К_{СА}$ – коэффициент укомплектованности штатных должностей системными администраторами системы защиты информации и кибербезопасности ОКИИ;

$Ш_{СА}$ – штатная численность должностей системных администраторов системы защиты информации и кибербезопасности ОКИИ;

$Ф_{СА}$ – фактически имеющаяся численность системных администраторов системы защиты информации и кибербезопасности ОКИИ.

Оценивания способности укомплектованности штатных должностей системными администраторами оказывать влияние на $Э_{СЗИКБ}$ предлагается осуществлять по критериям наведённых в табл. 4.

Таблица 4. *Критерии оценивания способности укомплектованными штатными должностей системными администраторами критически оказывать влияние на* $Э_{СЗИКБ}$

Критерий эффективности $Э_{СЗИКБ}$	коэффициент укомплектованности штатных должностей системными администраторами				
	$0 \le К_{СА} \le 0,25$	$0,25 < К_{СА} \le 0,5$	$0,5 < К_{СА} \le 0,75$	$0,75 < К_{СА} \le 0,9$	$0,9 < К_{СА} \le 1$
	Очень низкий (ОН)	Низкий (Н)	Средний (С)	Высокий (В)	Очень высокий (ОВ)
$0 \le Э_{СЗИКБ} \le 0,25$	ОН	ОН	ОН	ОН	ОН
$0,25 < Э_{СЗИКБ} \le 0,5$	Н	Н	Н	Н	Н
$0,5 < Э_{СЗИКБ} \le 0,75$	С	С	С	С	С
$0,75 < Э_{СЗИКБ} \le 0,9$	С	С	С	В	В
$0,9 < Э_{СЗИКБ} \le 1$	В	В	В	В	ОВ

Расчет коэффициента укомплектованности штатных должностей обслуживающим персоналом системы защиты информации и кибербезопасности ОКИИ осуществляется по формуле (7):

$$К_{ОП} = \frac{Ф_{ОП}}{Ш_{ОП}} \quad (7)$$

где $К_{ОП}$ – коэффициент укомплектованности штатных должностей обслуживающим персоналом системы защиты информации и кибербезопасности ОКИИ;

$Ш_{ОП}$ – штатная численность должностей обслуживающего персонала системы защиты информации и кибербезопасности ОКИИ;

$Ф_{ОП}$ – фактически имеющаяся численность обслуживающего персонала системы защиты информации и кибербезопасности ОКИИ.

Оценивания способности укомплектованности штатных должностей обслуживающим персоналом оказывать влияние на $Э_{СЗИКБ}$ предлагается осуществлять по критериям наведённых в табл. 5.

Таблица 5. *Критерии оценивания способности укомплектованными штатными должностей обслуживающим персоналом критически оказывать влияние на* $Э_{СЗИКБ}$

Критерий эффективности $Э_{СЗИКБ}$	коэффициент укомплектованности штатных обслуживающим персоналом				
	$0 \le К_{ОП} \le 0,25$	$0,25 < К_{ОП} \le 0,5$	$0,5 < К_{ОП} \le 0,75$	$0,75 < К_{ОП} \le 0,9$	$0,9 < К_{ОП} \le 1$
	Очень низкий (ОН)	Низкий (Н)	Средний (С)	Высокий (В)	Очень высокий (ОВ)
$0 \le Э_{СЗИКБ} \le 0,25$	ОН	ОН	ОН	ОН	ОН
$0,25 < Э_{СЗИКБ} \le 0,5$	Н	Н	Н	Н	Н
$0,5 < Э_{СЗИКБ} \le 0,75$	С	С	С	С	С
$0,75 < Э_{СЗИКБ} \le 0,9$	С	С	С	В	В
$0,9 < Э_{СЗИКБ} \le 1$	В	В	В	В	ОВ

Математическая модель расчета эффективности функционирования системы защиты информации и кибербезопасности ОКИИ по критерию выявленных активных угроз по результатам penetration testing. Данный подход видит цель контроль киберзащищённости средств и их

компонентов ОКИИ состоянию на момент времени $t_{ДИВ1}$ за условий действий тестовых деструктивных информационных влияний (ДИВ) ($F_{ДЕВ}$=1).

Если в ОКИИ есть средства (компонента) активного противодействия кибервлянию, то в таком случае исчисление $P_{КЗ}(S)$ осуществляется с использованием показателей удачных и неудачных попыток нарушения нормального функционирования указанного средства. Расчет киберзащищённости $P_{КЗ}(S)$ системы S осуществляется по формуле (8):

$$\mathrm{P}_{\mathrm{КЗ}}^{\mathrm{РТ}}(S) = 1 - \frac{N_{\mathrm{ДИВ}}^{\mathrm{Удачных}}(S)}{N_{\mathrm{ДИВ}}^{\mathrm{Общ}}(S)} \quad (8)$$

где $N_{\mathrm{ДИВ}}^{\mathrm{Общ}}(S)$ – общее количество проведенных ДИВ на всю систему S;

$N_{\mathrm{ДИВ}}^{\mathrm{Удачных}}(S)$ – количество удачных попыток реализации ДИВ на всю систему S по результатам оповещение системой фиксирования инцидентов.

Система S будет считается такой, что прошла проверку контроля на киберзащищённость, если по результатам расчета киберзащищённости по состоянию на время $t_{FДИВ1}$ при $F_{ДИВ}$ =1 удовлетворило критерии табл. 6.

Таблица 6. *Критерии оценки киберзащищённости ОКИИ по результатам penetration testing*

Критерий эффективности	Уровень	Лингвистическое описание уровня киберзащищённости
$0{,}9 < P_{КЗ}^{РТ}(S) \leq 1$	очень высокий	очень высокий уровень киберзащищённости, ДИВ практически никогда не будет проведена
$0{,}75 < P_{КЗ}^{РТ}(S) \leq 0{,}9$	высокий	высокий уровень киберзащищённости, вероятность проведения ДИВ достаточно низкая
$0{,}5 < P_{КЗ}^{РТ}(S) \leq 0{,}75$	средний	средний уровень киберзащищённости, вероятность проведения ДИВ средняя
$0{,}25 < P_{КЗ}^{РТ}(S) \leq 0{,}5$	низкий	низкий уровень киберзащищённости, вероятность проведения ДИВ скорее всего будет проведена
$0 \leq P_{КЗ}^{РТ}(S) \leq 0{,}25$	очень низкий	очень низкий уровень киберзащищённости, вероятность проведения ДИВ почти наверняка будет проведена

Обобщение результатов вычисления эффективности функционирования системы защиты информации и кибербезопасности.

Сводная таблица значений эффективности по критериям представлены в табл. 7.

Таблица 7. *Сводная таблица значений по показателям эффективности* $Э_{СЗИКБ}$

Обобщённый показатель эффективности $Э_{СЗИКБ}$	Частные показатели эффективности						
	$P_{КЗ}$	$K_{УС}$	$K_{ТГС}$	$K_{УИС}$	$K_{СА}$	$K_{ОП}$	$P_{КЗ}^{РТ}(S)$
очень низкий							
низкий							
средний							
высокий							
очень высокий							

Обобщённый показатель эффективности функционирования системы защиты информации и кибербезопасности ОКИИ предлагается определить, как средне арифметическую сумму частных показателей (9):

$$Э_{СЗИКБ} = \frac{P_{КЗ} + K_{УЗ} + K_{УИС} + K_{СА} + K_{ОП} + P_{КЗ}^{РТ}(S)}{7}. \quad (9)$$

Если по отдельному показателю не осуществлялось вычисление, то в расчётную формулу (9) не подставляются соответствующие значения, а в выводах указывается краткое обоснование почему не использовался показатель. Критерии оценки эффективности функционирования системы защиты информации и кибербезопасности ОКИИ по обобщенном показателе представлены в табл. 8.

Таблица 8. *Критерии оценки эффективности функционирования системы защиты информации и кибербезопасности ОКИИ по обобщенном показателю* $Э_{СЗИКБ}$

Критерий $Э_{СЗИКБ}$	Уровень	Лингвистическое описание	
$0 \le Э_{СЗИКБ} \le 0{,}25$	очень низкий	неудовлетворительный уровень эффективности	Утечка информации и кибернезахищена
$0{,}25 < Э_{СЗИКБ} \le 0{,}5$	низкий	низкий уровень эффективности	Создания условий для утечки информации и кибе рыску
$0{,}5 < Э_{СЗИКБ} \le 0{,}75$	средний	средний уровень эффективности	Обеспечения гарантированной защиты информации и кибербезопасности
$0{,}75 < Э_{СЗИКБ} \le 0{,}9$	высокий	в целом высокий уровень эффективности	
$0{,}9 < Э_{СЗИКБ} \le 1$	очень высокий	наивысший уровень эффективности	

ВЫВОДЫ

Безусловно количественная оценка эффективности функционирования системы защиты информации и кибербезопасности ОКИИ требует больших усилий, чем использование качественных методов. Однако и отдача прежде всего экономически, будет гораздо весомее, а интересы, как заказчика и разработчика системы защиты информации и кибербезопасности ОКИИ, будут заниженными более надежно.

Учитывая выше подходов и критериев на современном этапе развития видится рациональным применять не все, а наиболее показательные подходы, которые позволяют наглядно продемонстрировать эффективности функционирования системы защиты информации и кибербезопасности ОКИИ.

НАУЧНАЯ НОВИЗНА

Научная новизна полученного результата заключается в том, что предложено показатели и математические критерии возможной оценки эффективности функционирования системы защиты информации и кибербезопасности в ОКИИ.

ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ НАУЧНЫХ ИССЛЕДОВАНИЙ

Представленное исследование не исчерпывает всех аспектов обозначенной проблемы. Теоретические и практические результаты, полученные в процессе научного поиска, составляют основу для дальнейшего обоснования методики оценки эффективности функционирования системы защиты информации и кибербезопасности в ОКИИ.

СПИСОК ЛИТЕРАТУРЫ

1. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем // Искусственный интеллект. 2008. № 4.С. 253 – 264.
2. Андреев К. Метод оценки экономической эффективности подразделения по защите информации // Информационная безопасность. 2010. № 5. URL: http://www.itsec.ru/ articles2/Oborandteh/metod-ocenki-ekonomicheskoi-effektivnosti-podrazdeleniya-po-zashite-informacii (дата обращения 7.12.2021).
3. Ефимов Е.Н., Лапицкая Г.М. Оценка эффективности мероприятий информационной безопасности в условиях неопределенности // Бизнес-информатика. 2015. №1(31). С. 51–57.
4. Zabara S., Kozubtsova L., Kozubtsov I. Improved method of diagnostics of cyber security of the information system taking into account disruptive cyber impacts // «Danish Scientific Journal» (DSJ). Kobenhavn. Denmark. 2020. Vol. 35(1). Pp. 68 – 74. ISSN 3375-2389.
5. Козубцова Л.М. Удосконалена методика діагностування кібернетичної захищеності інформаційної системи з урахуванням деструктивних кібернетичних впливів // Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво». Луцьк, 2020. Випуск № 39. С. 127 – 135.