Scientific and Practical Cyber Security Journal (SPCSJ) 6(3): 13-24 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И КИБЕРБЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

PERFORMANCE INDICATORS OF FUNCTIONING OF THE INFORMATION PROTECTION AND CYBER SECURITY SYSTEM OF OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

Черноног Александр Александрович, Директорат политики цифровой трансформации и информационной безопасности в сфере обороны, Министерство обороны Украины, Киев, Украина
Oleksandr Chernonoh, Directorate of digital transformation and information security policy in the field of Defense, Ministry of defense of Ukraine, Kiev, Ukraine
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
д.п.н., профессор Козубцов Игорь Николаевич, Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Doctor of Pedagogical Sciences, Professor, Igor Kozubtsov, Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
к.т.н., доцент Здолбицкая Нина Васильевна, Луцкий национальный технический университет, г. Луцк, Украина
Candidate of Engineering Sciences, associate professor Nyna Zdolbytskaia, Lutsk National Technical University, Lutsk, Ukraine
к.т.н., Кошелюк Виктор Андреевич, Луцкий национальный технический университет, г. Луцк, Украина
Candidate of Engineering Sciences, Vyktor Kosheliuk, Lutsk National Technical University, Lutsk, Ukraine
к.т.н., Штаненко Сергей Станиславович, Военный институт телекоммуникаций и информатизации имени Героев Крут, г. Киев, Украина
Candidate of Engineering Sciences, associate professor Sergei Sctanenko, Military institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine

АННОТАЦИЯ. В научной статье решена частная научно-техническая проблема по необходимости выбора возможных показателей эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры. Научная новизна полученного результата заключается в том, что впервые предложены непротиворечивые показатели и критерии оценивания эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры. Практическое значение работы заключается в том, что на основе полученных показателей и критериев в дальнейшей работе на их основании разработать частную методику оценки эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры.

КЛЮЧЕВЫЕ СЛОВА: *показатели, критерии, оценки, эффективность, функционирование, система защиты информации и кибербезопасности, объекты критической информационной инфраструктуры*.

ABSTRACT. The scientific article solves a private scientific and technical problem of the need to select possible indicators of the effectiveness of the information security system and cybersecurity of critical information infrastructure facilities. The scientific novelty of the obtained result lies in the fact that for the first time consistent indicators and criteria for evaluating the effectiveness of the information security system and cybersecurity of critical information infrastructure objects are proposed. The practical significance of the work lies in the fact that, based on the obtained indicators and criteria, in further work on their basis, to develop a private methodology for evaluating the

effectiveness of the information security system and cybersecurity of critical information infrastructure facilities.

KEYWORDS: *indicators, criteria, assessments, efficiency, functioning, information security and cybersecurity system, critical information infrastructure facilities*.

ВВЕДЕНИЕ

Постановка задачи и связь ее с важными научными задачами. Система защиты информации и кибербезопасности объектов критической информационной инфраструктуры (СЗИКБ ОКИИ) – это сложный комплекс программных, криптографических, организационных и других средств, методов и мероприятий, предназначенных для защиты информации и кибербезопасности [1]. От уровня обеспечения зависит значение эффективности функционирования СЗИКБ ОКИИ. Без преувеличения зависит безопасность любого государства. В связи с этим возникает научная задача каким образом и по каким показателям оценить эффективно ли функционирует построенная и настроенная СЗИКБ ОКИИ.

Отсутствие единой методологии оценивания эффективности функционирования СЗИКБ ОКИИ приводит к нерациональным шагам по модернизации и усовершенствованию, чрезмерной необоснованной закупки «новых» программных, программно-аппаратных комплексов, криптографических, организационных и других средств, методов и мероприятий, предназначенных для защиты информации и кибербезопасности. Эта научно-техническая проблема возникла вследствии противоречия:

в необходимости иметь СЗИКБ ОКИИ, относительно новой системы, которой ранее не существовало прототипа;

в отсутствии единого подхода и методологии оценивания эффективности функционирования СЗИКБ ОКИИ.

Для решения противоречивых составляющих общей проблемы, сформулируем научную задачу исследования: определить и обосновать вероятностно возможные показатели, по которым возможно объективно определять некую эффективность функционирования СЗИКБ ОКИИ.

АНАЛИЗ ИССЛЕДОВАНИЙ И ПУБЛИКАЦИЙ

В работе [2] для оценки эффективности системы защиты информационной системы, автор применял показатель *E* степень достижения цели этой системой.

В работе [3] автором для оценки эффективности подразделений защиты информации применялись показатели экономической эффективности.

В условиях неопределенности [4] авторы придерживаются единого мнения и используют математическую модель оценки эффективности функционирования системы по критерию предотвращения потерь. По сути, ЗВ является разницей потерь до и после реализации мероприятий, направленных на повышение уровня информационной или кибербезопасности, и в целом отражает ту часть прибыли, которая могла быть потеряна.

Применение данного подхода затруднено вследствие отсутствия подходов к расчету В1 и В2. В связи с этим актуализируется сформулированная новая научная задача.

Предложенная в работе [5] методика обеспечивает вычисление и оценки эффективности выполнения мероприятий обеспечения кибербезопасности объектов критической информационной инфраструктуры организаций.

В авторской работе [6] эффективность функционирования системы защиты информации и кибербезопасности, определялась по показателям: киберзащищенности; коэффициентом укомплектованности средствами криптографической защиты информации, технической защиты информации и киберзащиты; коэффициентом технической готовности средств криптографической защиты информации, технической защиты информации и киберзащиты; коэффициентом укомплектованности исправными средствами криптографической защиты информации, технической защиты информации и киберзащиты; коэффициентом укомплектованности штатных должностей системными администраторами; коэффициентом укомплектованности штатных должностей обслуживающим персоналом; киберзахищенностью по результатам penetration testing.

Таким образом с анализа последних исследований и публикаций по данному направлению исследований можно сделать выводи:

1) решаемая проблема не является новой, а вот результат исследования может отображать новое решение;

2) решение научной задачи является приоритетным направлением исследований [1] не только для Украины, но для многих развивающихся стан.

ЦЕЛЬ СТАТЬИ

Охарактеризовать математические показатели и критерии такого оценивания эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры.

ОСНОВНОЙ РЕЗУЛЬТАТ ИССЛЕДОВАНИЯ

Под «эффективностью СЗИКБ ОКИИ» ($E_{СЗИКБ}$) в данном исследовании будем понимать степень соответствия достигнутых результатов поставленным целям по защите информации.

Оценка эффективности может осуществляться в процессе создания, приемки и эксплуатации СЗИКБ. Ключевым понятием является критерий оценки – признак, основание принятия решения по оценке эффективности на соответствие выдвинутым требованиям. Для осуществления такой оценки нужны объективные показатели эффективности.

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

К показателям эффективности выдвигаются следующие требования:

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.).

Согласно принятого нами определения эффективности ($E_{П(СЗИКБ)}$) в подготовке решения задачи было изучено дополнительно мировой опыт и рекомендации руководящих документов [7-17]. Результатом синтетической переработки нами предлагаются множество показателей эффективности. Их числовые значения величин, примем для характеристики (описания) степени достижения исследуемой системой защиты информации и кибербезопасности, поставленных перед ней задач.

Система связи показателей $E_{(СЗИКБ)}$ эффективности СЗИКБ ОКИИ составлен для наглядности в табличной форме (табл. 1).

Таблица 1. Система связи показателей $E_{(СЗИКБ)}$ эффективности СЗИКБ ОКИИ

Показатели $E_{П(СЗИКБ)}$	Частичные показатели $E_{ЧП(СЗИКБ)}$	Индикаторы частичных показателей ($И_{Ч(СЗИКБ)}$)
ID. Идентификация рисков кибербезопасности	ID. AM. Управление активами	ID. AM-1. Физическое оборудование и системы на ОКИ идентифицированы и задокументированы. ID. AM-2. Программное обеспечение, используемые ОКИ для предоставления жизненно важных услуг и функций, идентифицированы и задокументированы. ID. AM-3. Телекоммуникации и потоки данных ОКИ идентифицированы и задокументированы. ID. AM-4. Внешние информационные и информационно-телекоммуникационные системы, промышленные системы, которые взаимодействуют с информационно-телекоммуникационными и другими системами ОКИ учтено. ID. AM-5. Критичность активов (оборудования, данных, программного обеспечения) ОКИ определен согласно оценке их влияния, на предоставление жизненно важных услуг и функций ОКИ.

		ID. AM-6. Обязанности штатного персонала ОКИ и партнеров организации (например, поставщиков, клиентов, и т.п.) обеспечения кибербезопасности и в определенно и закреплено в соответствующих документах.
	ID. BE. Среда предоставления жизненно важных услуг и функций	ID. BE-1. Роль ОКИ в цепи поставки товаров и услуг определено и сообщено всем поставщикам организации. ID. BE-2. Место и роль ОКИ в системе оказания жизненно важных услуг и функций сектору (подсектору) критической инфраструктуры определено и сообщено всем поставщикам организации. ID. BE-3. Приоритетность целей, задач и мероприятий по обеспечению кибербезопасности предоставления жизненно важных услуг и функций установлено и сообщено. ID. BE-4. Зависимости и важнейшие процессы для обеспечения предоставления жизненно важных услуг и функций установлено. ID. BE-5. Требования к устойчивости ОКИ по обеспечению предоставления жизненно важных услуг и функций установлено.
	ID. GV. Управление безопасностью	ID. GV-1. Правила (политики) кибербезопасности ОКИ установлены и задокументированы. ID. GV-2. Обязанности по обеспечению кибербезопасности ОКИ скоординировано и согласовано с обязанностями персонала ОКИ и с внешними партнерами. ID. GV-3. Правовые и нормативные требования по обеспечению кибербезопасности ОКИ, в том числе обязательства по защите неприкосновенности частной жизни (приватности), осознано и управление ими осуществляется. ID. GV-4. Процессы управления безопасностью и управление рисками направлено на решение вопроса обработки рисков кибербезопасности.
	ID. RA. Оценка рисков	ID. RA-1. Уязвимости активов ОКИ проанализированы, было выявлено и задокументировано. ID. RA-2. Информация об угрозах безопасности и уязвимости получена с форумов обмена информацией и официальных источников. ID. RA-3. Угрозы кибербезопасности (модель угроз) как внутренние, так и внешние определены и задокументированы. ID. RA-4. Потенциальные последствия (уровень ущерба), которые могут нанести угрозы в следствие их реализации на непрерывное предоставление жизненно важных услуг и функций, и вероятности их реализации определен. ID. RA-5. Для определения риска применяются данные относительно угроз, уязвимостей, их вероятностей и уровня ущерба использовано для

		определения риска кибербезопасности. ID. RA-6. Меры реагирования на риск кибербезопасности определены и их приоритетность установлено.
	ID. RM. Стратегия управления рисками организации	ID. RM-1. Процессы управления рисками определены, согласованы с партнерами организации и управляются. ID. RM-2. Допустимый уровень риска кибербезопасности определено и четко выражено. ID. RM-3. Определение допустимого уровня риска основывается на роли ОКИ как составной части сектора критической инфраструктуры и анализе рисков, присущих соответствующему сектору критической инфраструктуры.
	ID. SC. Управления рисками системы снабжения	ID. SC-1. Процессы управления рисками кибербезопасности системы снабжения определено, согласовано с партнерами организации и управляются. ID. SC-2. Поставщики (распорядители) информационных систем, товаров и услуг для ОКИ идентифицировано, уровень их критичности оценены в соответствии с политикой управления рисками кибербезопасности с учетом рисков, присущих системе снабжения. ID. SC-3. Поставщики товаров и услуг, партнеры, в соответствии с договором, могут внедрять мероприятия, направленные на достижение цели политики информационной безопасности/кибербезопасности ОКИ и плана управления рисками поставки. ID. SC-4. С поставщиками осуществляется планирование и тестирование реагирования по соответствующим политикам реагирования на киберинциденты и восстановление состояния кибербезопасности.
PR. Киберзащита	PR. AC. Управление идентификацией, аутентификацией и контроль доступа	PR. AC-1. Идентификаторы и данные для проверки подлинности авторизованных пользователей, администраторов и процессов назначаются, верифицируются, администрируются, отзываются (отменяются) и проверяются. PR. AC-2. Физический доступ к ОКII защищен и управляется. PR. AC-3. Осуществляется контроль и управление удаленного доступа. PR. AC-4. Права доступа установлены с применением принципов минимальных привилегий и распределения обязанностей. PR.AC-5. Целостность телекоммуникационной сети защищено (например, сегментация сети). PR.AC-6. Аутентификация пользователей, администраторов, устройств и других активов осуществляется (например методами однофакторной, многофакторной проверки подлинности) в соответствии с установленным

		риском нарушения безопасности.
	PR. AT. Осведомленность и обучение	PR. AT-1. Все сотрудники ОКИ знакомы и прошли подготовку по вопросам кибербезопасности. PR. AT-2. Пользователи (администраторы) с преимуществами доступа понимают свои обязанности по вопросам кибербезопасности. PR. AT-3. Партнеры организации понимают свои обязанности по вопросам кибербезопасности. PR. AT-4. Руководство ОКИ понимает свои обязанности по вопросам кибербезопасности. PR. AT-5. Персонал по обеспечению физической и информационной безопасности понимает свои обязанности.
	PR. DS. Безопасность данных	PR. DS-1. Данные, которые хранятся, защищены. PR. DS-2. Данные, передаваемые защищены. PR. DS-3. Управление активами осуществляется соблюдением правил удаления, передачи и размещения. PR. DS-4. Необходимые способности для обеспечения доступности активов созданы и поддерживаются. PR. DS-5. Защита от утечки данных внедрено. PR. DS-6. Механизмы проверки целостности используются для верификации программного обеспечения, программно-аппаратных средств и целостности информации. PR. DS-7. Среды разработки тестирование отделены от производственной среды.
	PR. IP. Процессы и процедуры киберзащиты	PR. IP-1. Базовая конфигурация информационно-телекоммуникационных систем/систем управления производственными процессами создана и поддерживается. PR. IP-2. Жизненный цикл разработки, эксплуатации и управления системами (SDLC) внедрена. PR. IP-3. Процессы (мероприятия) управление изменениями конфигурации внедрено. PR. IP-4. Резервное копирование информации производится, поддерживается и периодически тестируется. PR. IP-5. Правила (политика) и нормы физической безопасности операционной среды и оборудования организации (ОКИ) выполняются. PR. IP-6. Данные уничтожаются согласно политике безопасности. PR. IP-7. Процессы киберзащиты постоянно совершенствуются. PR. IP-8. Планы реагирования (реагирования на киберинциденты и обеспечения непрерывности бизнеса и планы восстановления (восстановление после киберинцидента и восстановления после аварии) имеющиеся и управляются. PR.IP-9. Планы реагирования и восстановления тестируются. PR.IP-10. План управления уязвимостями

		разработано и внедрено.
	PR. MA. Техническое обслуживание	PR. MA-1. Техническое обслуживание и ремонт активов ОКИ выполняются своевременно документируются с использованием определенных и контролируемых средств. PR. MA-2. Дистанционное обслуживание активов ОКИ одобрено, задокументировано и выполняется способом, что делает невозможным несанкционированный доступ.
	PR. PT. Технологии киберзащиты	PR. PT-1. Записи аудита (журналов событий) определены, задокументированы, внедрены и проверены в соответствии с политиками, правилами, процедурами по безопасности. PR. PT-2. Сменные носители защищены, а их использование ограничено в соответствии с правилами, процедур по безопасности. PR. PT-3. Контроль доступа к системам и активам осуществляется с применением принципа минимальных привилегий. PR. PT-4. Телекоммуникационные сети и сети управления защищены. PR. PT-5. Внедрение механизмов на ОКИ для достижения требований к устойчивости в случае чрезвычайных ситуаций и инцидентов в киберпространстве.
DE. Выявления киберинцидентов	DE. AE. Аномалии и киберинциденты	DE. AE-1. Эталоны сетевых операций и ожидаемых потоков данных для пользователей и систем установлены и управляются. DE. AE-2. Существует практика анализа выявленных событий. DE. AE-3. Данные о киберинциденты агрегируются и коррелируются с нескольких источников и датчиков. DE. AE-4. Существует процесс определения возможных воздействий киберинцидентов. DE. AE-5. Пороги оповещения о киберинцидентах встановлено.
	DE. CM. Непрерывный мониторинг кибербезопасности	DE. CM-1. Телекоммуникационная сеть (ОКИИ) отслеживается для выявления потенциальных киберинцидентов. DE. CM-2. Физическая среда отслеживается для выявления потенциальных киберинцидентов. DE. CM-3. Активность персонала отслеживается для выявления потенциальных киберинцидентов. DE. CM-4. Вредоносный код обнаруживается. DE. CM-5. Несанкционированный программный продукт обнаружено. DE. CM-6. Активность внешнего поставщика товаров и услуг отслеживается с целью выявления потенциальных киберинцидентов. DE.CM-7. Мониторинг неавторизованного персонала, соединений, устройств и программного обеспечения осуществляется на постоянной основе. DE.CM-8. Сканирование уязвимостей выполняется

	DE. DP. Процессы обнаружения киберинцидентов	DE. DP-1. Обязанности по выявлению киберинцидентов четко определено для обеспечения отчетности. DE. DP-2. Меры выявления киберинцидентов соответствуют всем применимым требованиям. DE. DP-3. Процессы выявления киберинцидентов протестированы. DE. DP-4. Информация о выявленных киберинцидентах сообщена партнерам организации. DE. DP-5. Процессы выявления киберинцидентов постоянно совершенствуются.
RS. Реагирование на киберинциденты	RS. RP. Планирование реагирования	RS. RP-1. План реагирования выполняется во время или после события.
	RS. CO. Коммуникации	RS. CO-1. Персонал знает свои обязанности и порядок действий в ситуациях, когда необходимо реагирование на киберинциденты. RS. CO-2. Факты о киберинцидентах задокументированы и сообщаются в соответствии с установленными критериями. RS. CO-3. Осуществляется обмен информацией о киберинцидентах в соответствии с планами реагирования. RS. CO-4. Координация с партнерами организации проводится в соответствии с планами реагирования. RS. CO-5. С целью достижения более широкой ситуативной осведомленности относительно состояния кибербезопасности осуществляется обмен информацией с основными субъектами национальной системы кибербезопасности и внешними партнерами организации.
	RS. AN. Анализ	RS. AN-1. Сообщение от систем обнаружения киберинцидентов исследуются. RS. AN-2. Влияние киберинцидентов осознано. RS. AN-3. Киберинциденты классифицированы в соответствии с планами реагирования. Электронные доказательства собираются и фиксируются должным образом. RS. AN-4. Создано процессы для получения анализа и реагирования на факторы уязвимости, обнаруженные организацией из внутренних и внешних источников.
	RS. MI. Минимизация последствий.	RS. MI-1. Киберинциденты устранены. RS. MI-2. Последствия киберинцидентов минимизировано. RS. MI-3. Впервые обнаруженные уязвимости устранены или задокументировано как принятые риски.
	RS. IM. Усовершенствования	RS.IM-1. В планах реагирования учтен полученный опыт. RS.IM-2. Планы реагирования обновлен.
RC. Восстановление состояния кибербезопасности	RC. RP. Планирование восстановления	RC. RP-1. План восстановления выполняется во время или после киберинцидентов.
	RC. IM. Усовершенствования	RC. IM-2. План восстановления обновлен. RC. IM-1. Планы восстановления учитывают

		полученный опыт.
	RC. CO. Коммуникации	RC. CO-1. Процесс связей с общественностью организован и является управляемым. RC. CO-2. Репутация после киберинцидентов восстанавливается. RC. CO-3. Меры по восстановлению сообщены внутренним и внешним партнерам организации, а также руководству.

Критерии оценки эффективности функционирования СЗИКБ ОКИИ.

Для оценки индикаторов частичных показателей $И_{ЧП(СЗИКБ)}$ рекомендуем применять следующие критерии табл. 2.

Таблица 2. Критерии оценивания индикаторов частных показателей $И_{ЧП(СЗИКБ)}$

Критерий $И_{ЧП(СЗИКБ)}$	Уровень
$И_{ЧП(СЗИКБ)}= 0$	не реализовано функцию
$И_{ЧП(СЗИКБ)} = 1$	реализована функция

Для оценки частичных показателей $Е_{ЧП(СЗИКБ)}$ рекомендуем применять следующие критерии табл. 3.

Таблица 3. Критерии оценивания частных показателей $Е_{ЧП(СЗИКБ)}$

Критерий $Е_{ЧП(СЗИКБ)}$	Уровень
$0 \le Е_{ЧП(СЗИКБ)} \le 0,25$	неудовлетворительное (НЗ)
$0,25< Е_{ЧП(СЗИКБ)} \le 0,5$	низкий (Н)
$0,5< Е_{ЧП(СЗИКБ)} \le 0,75$	средний (С)
$0,75< Е_{ЧП(СЗИКБ)} \le 0,9$	высокий (В)
$0,9< Е_{ЧП(СЗИКБ)} \le 1$	высокий (НВ)

Для оценки показателей $Е_{П(СЗИКБ)}$ рекомендуем применять следующие критерии табл. 4.

Таблица 4. Критерии оценивания показателей $Е_{П(СЗИКБ)}$

Критерий $Е_{П(СЗИКБ)}$	Уровень
$0 \le Е_{П(СЗИКБ)} \le 0,25$	неудовлетворительное (НЗ)
$0,25< Е_{П(СЗИКБ)} \le 0,5$	низкий (Н)
$0,5< Е_{П(СЗИКБ)} \le 0,75$	средний (С)
$0,75< Е_{П(СЗИКБ)} \le 0,9$	высокий (В)
$0,9< Е_{П(СЗИКБ)} \le 1$	высокий (НВ)

Критерии оценки эффективности функционирования СЗИКБ ОКИИ по обобщенному показателю представлены в табл. 5.

Таблица 5. Критерии оценки эффективности функционирования СЗИКБ ОКИИ по обобщенным показателем

Критерий $Е_{П(СЗИКБ)}$	Уровень
$0 \le Е_{СЗИКБ} \le 0,25$	Частичный
$0,25< Е_{СЗИКБ} \le 0,5$	Риск ориентирований
$0,5< Е_{СЗИКБ} \le 0,75$	Повторяющийся
$0,75< Е_{СЗИКБ} \le 1$	Адаптивный

Лингвистическое описание частичного уровня. **Практика киберзащиты.** Практическая деятельность по реализации мер киберзащиты и управлению рисками кибербезопасности не является формализованной. Деятельность по внедрению мер киберзащиты и управлению рисками носит произвольный и ситуативный характер. Приоритетность выполнения мероприятий киберзащиты непосредственно не учитывает цели

ОКИИ по управлению рисками, характеристики угроз, задачи по предоставлению жизненно важных услуг и функций.

Политика управления рисками. Ограниченное понимание риска кибербезопасности на организационном уровне. Информированность руководства и персонала организации о рисках кибербезопасности является недостаточной. Общий подход к управлению рисками кибербезопасности в масштабе всего ОКИИ не установлен. Меры киберзащиты внедряются нерегулярно, ситуативно, используя разнообразный практический опыт или информацию, полученную из внешних источников. Процессов, обеспечивающих внутренний обмен информацией о состоянии кибербезопасности, не зафиксировано.

Взаимодействие с другими ОКИ. Организация не понимает свою роль в экосистеме в отношении своих собственных зависимостей или зависимых от нее других субъектов. Организация не обрабатывает или получает информацию (исследования угроз, лучшие практики, технологии) от других организаций (потребители, поставщики, зависимые от нее или организаций, от которых она зависит, организаций анализа и распространения информации, исследователи, государственные органы) и не распространяет такую информацию. Организация вообще не осознает рисков кибербезопасности, связанных с услугами, которые она предоставляет и которыми пользуется.

Лингвистическое описание рискориентированного уровня. **Практика киберзащиты.** Практика реализации мер киберзащиты и управления рисками утверждается руководством организации, но может не устанавливаться как общая политика для организации. Приоритетность деятельности по кибербезопасности и потребности защиты напрямую зависят от целей организационного риска, среды угроз или требований по предоставлению жизненно важных услуг и функций.

Политика управления рисками. Существует осознание риска кибербезопасности на организационном уровне, но общий подход организации к управлению риском кибербезопасности не установлено. Информация о кибербезопасности распространяется в рамках организации на неофициальной основе. Рассмотрение кибербезопасности в целях и программах организации может происходить на некоторых, но не на всех уровнях организации. Оценка рисков кибербезопасности для организационных и внешних активов происходит, но обычно не повторяется или одинаково не проводится.

Взаимодействие с другими ОКИ. В целом организация понимает свою роль в экосистеме в отношении своих собственных зависимостей или зависимых от нее других субъектов, но не обоих. Организация обрабатывает и получает некоторую информацию от других организаций, создает на основании нее собственную информацию, но может не распространять такую информацию между другими организациями. Кроме того, организация осознает риски кибербезопасности, связанные с услугами, которые она предоставляет и которыми пользуется, но не действует последовательно или по утвержденным правилам.

Лингвистическое описание повторяющегося уровня. **Практика киберзащиты.** Практика реализации мер киберзащиты и управления рисками в организации является официально утвержденной и определена как политика. Результаты киберзащиты регулярно отслеживаются и меры киберзащиты регулярно обновляются на основе применения процессов управления рисками к изменениям в требованиях по предоставлению жизненно важной функции, меняющихся угроз и технологического ландшафта.

Политика управления рисками. В организации существует общий подход к управлению рисками кибербезопасности. Политики информирования о рисках, процессах и процедурах определены, реализуются по назначению и пересматриваются. Существуют последовательные методы эффективного реагирования на изменения риска. Персонал обладает знаниями и умениями выполнять назначенные им обязанности. Организация последовательно и точно контролирует риск кибербезопасности для активов организации. Связанные и не связанные с кибербезопасностью главные исполнители регулярно общаются о риске кибербезопасности.

Взаимодействие с другими ОКИ. Организация понимает свою роль в экосистеме в

отношении своих собственных зависимостей или зависимых от нее других субъектов и может способствовать более широкому пониманию сообществом рисков. Организация регулярно обрабатывает и получает информацию от других организаций, что дополняет собственную созданную информацию и распространяет ее между другими организациями. Организация осознает риски кибербезопасности, связанные с услугами, которые она предоставляет и которыми пользуется.

Лингвистическое описание адаптивного уровня. **Практика киберзащиты.** Организация адаптирует свою практику в области кибербезопасности на основе предыдущих и текущих мероприятий по кибербезопасности, включая полученные результаты и прогнозные показатели. Благодаря процессу непрерывного совершенствования, что предполагает передовые технологии и практики кибербезопасности, организация активно адаптируется в меняющихся киберугроз и своевременно и эффективно реагировать на киберугрозы, которые развиваются и усложняются.

Политика управления рисками. В организации существует общий подход к управлению риском кибербезопасности, который использует политику, процессы и процедуры с учетом рисков для решения потенциальных киберинцидентов. Взаимосвязь между риском кибербезопасности и целями организации четко осознается и учитывается при принятии решений. Главные исполнители контролируют риск кибербезопасности в том же контексте, что и финансовый риск, и другие риски для организации. Управление рисками кибербезопасности является частью организационной культуры и развивающийся на основе осознания предыдущей деятельности и постоянного осознания деятельности в своих системах и телекоммуникационных сетях. Организация может быстро и эффективно учитывать изменения в том, как подходить к обработке и сообщать о риске.

Взаимодействие с другими ОКИ. Организация понимает свою роль в экосистеме в отношении своих собственных зависимостей или зависимых от нее других субъектов, способствует более широкому пониманию сообществом рисков. Организация получает, создает и пересматривает приоритетную информацию для продолжения анализа этих рисков по мере развития ландшафта угроз и технологий. Организация распространяет эту информацию как внутри организации, так и снаружи для дальнейшей проработки. Организация использует информацию в режиме реального времени или почти в режиме реального времени и последовательно реагирует на риски кибербезопасности, связанные с услугами, которые она предоставляет и которыми пользуется.

ВЫВОДЫ

Таким образом, на современном этапе развития науки решена научно-техническая проблема с неопределенностью по каким показателям проводить процедуру оценивания выбора эффективность функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры. На данный момент усматривается при оценке эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры два ключевых показателя по функциональной способности и технической надежности.

В работе рассмотрено показатели оценивания по показателю функциональной способности.

НАУЧНАЯ НОВИЗНА

Впервые предложены показатели и критерии оценивания эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры.

ПРАКТИЧЕСКОЕ ЗНАЧЕНИЕ РАБОТЫ

На основании полученных показателей и критериев в дальнейших работах возникает возможность разработать методику оценки эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры.

ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ НАУЧНЫХ ИССЛЕДОВАНИЙ

Представленное исследование не исчерпывает всех аспектов указанной проблемы. Теоретические результаты, полученные в процессе научного поиска, составляют основу для

дальнейшего обоснования методики оценки эффективности функционирования системы защиты информации и кибербезопасности объектов критической информационной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ

1. Закон України “Про основні засади забезпечення кібербезпеки України”. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

2. Маслова Н.А. Методы оценки эффективности систем защиты информационны систем. Искусственный интеллект. 2008. № 4.С. 253–264.

3. 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.

4. Ефимов Е.Н., Лапицкая Г.М. Оценка эффективности мероприятий информационной безопасности в условиях неопределенности. Бизнес-информатика. 2015. №1(31). С. 51–57.

5. Козубцова Л.М., Хлапонин Ю.І., Козубцов І.М. Методика оцінювання ефективності виконання заходів забезпечення кібербезпеки об’єктів критичної інформаційної інфраструктури організацій. Сучасні інформаційні технології у сфері безпеки та оборони. 2021. №2(41). С. 17–22.

6. Козубцова Л.М., Рудоміно-Дусятська І.А., Сновида В.Є. Обчислення показників ефективності функціонування системи захисту інформації і кібербезпеки // Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво». Луцьк, 2021. Випуск №45. С. 19–25. URL: http://cit-journal.com.ua/index.php/cit/article/view/315/405.

7. International Energy Agency (2021) Enhancing Cyber Resilience in Electricity Systems. URL: https://webstore.iea.org/download/direct/4359.

8. International Organization for Standardization/International Electrotechnical Commission (2013) ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements (ISO, Geneva, Switzerland). URL: https://www.iso.org/standard/54534.html.

9. National Institute of Standards and Technology and North American Electric Reliability Corporation (2020) Mapping of NIST Cybersecurity Framework v1.1 to NERC CIP Reliability Standards. URL: https://doi.org/10.18434/mds2-2348.

10. North American Electric Reliability Corporation (2021) NERC CIP Enforceable Standards. URL: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

11. National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). URL: https://doi.org/10.6028/NIST.CSWP.04162018.

12. National Institute of Standards and Technology (2021) National Online Informative References Program. URL: https://csrc.nist.gov/projects/olir.

13. Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. URL: https://doi.org/10.6028/NIST.SP.800-53r4.

14. International Society of Automation (2013) ISA 62443-3-3:2013 – Security for industrial automation and control systems Part 3-3: System security requirements and security levels (ISA, North Carolina, USA). URL: https://www.isa.org/products/ansi-isa-62443-3-3-99-03-03-2013-security-for-indu.

15. Department of Energy (2021) Cybersecurity Capability Maturity Model. URL: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

16. Center for Internet Security (2021) CIS Controls V8. URL: https://www.cisecurity.org/controls/.

17. Information Systems Audit and Control Association (ISACA) (2021) Control Objectives for Information and Related Technologies. URL: https://www.isaca.org/resources/cobit.