Scientific and Practical Cyber Security Journal (SPCSJ) 2(4): 81-86 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

АНАЛИЗ СОВРЕМЕННЫХ ПОДХОДОВ К ОЦЕНИВАНИЮ ЗАЩИЩЕНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ГОСУДАРСТВА

Sergiy Gnatyuk, National Aviation University, Doctor of Science (Cybersecurity), Associate Professor, Kyiv, Ukraine
Viktoriia Sydorenko, National Aviation University, PhD in Information Security, Kyiv, Ukraine
Yuliia Polishchuk, National Aviation University, PhD Student, Kyiv, Ukraine
Vitaliy Kotelianets, National Aviation University, PhD Student, Kyiv, Ukraine

ABSTRACT. Currently, due to the large number of cyber incidents which occur daily, critical information infrastructure protection and assessing its security level is an important technical and scientific task. In this scientific paper, a qualitative analysis of well-known approaches and methods for assessment the security of information resources in critical information infrastructure objects is carried out. It will be useful for improving the level of critical information infrastructure protection of the state.

KEYWORDS: critical information infrastructure, security assessment method, cybersecurity, security of information resources.

Современное понятия критической информационной инфраструктуры (КИИ) выходит за рамки изучения лишь одной дисциплины. На сегодня, это сложная система, которая характеризуется совокупностью автоматизированных систем управления процессами критически важных объектов и систем, обеспечивающих их взаимодействие необходимых для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка. Именно поэтому, проблема обеспечения защищенности такой инфраструктуры является одним из наиболее актуальных вопросов, изучение которого требует системного подхода (Рис. 1). Исходя из того, что обеспечения безопасности объектов КИИ должно происходить на государственном уровне, государству необходимо обеспечить нормативно-правовую базу для регулирования вышеупомянутого вопроса. Для примера, рассматривая законодательную базу Украины, как и в большинстве пост-советских государств, на сегодня отсутствует методика оценивания защищенности информационных ресурсов (ИР) объектов КИИ, разработка которой безусловно есть актуальной научной задачей.

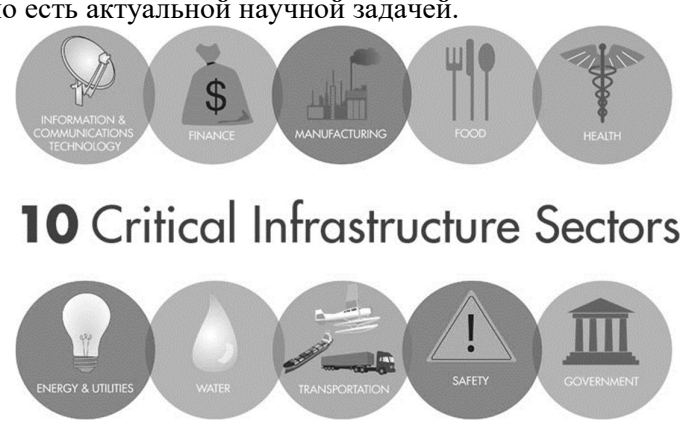

Рис. 1. Сектора КИИ согласно IPREM

В связи с этим, **целью настоящей работы** является проведения анализа современных подходов и методов для оценивания защищённости ИР объектов КИИ.

Основная часть. Проведя обзор подходов к оцениванию защищенности объектов КИИ, можно выделить следующие:

Украинский опыт

Приказом Администрации Государственной службы специальной связи и защиты информации Украины №112 от 2008 г. был утвержден Порядок оценки состояния защищенности государственных ИР в информационных, телекоммуникационных и информационно-телекоммуникационных системах (Порядок) [1]. Под процессом оценивания защищенности государственных ИР (процесс оценки) в информационных, телекоммуникационных и информационно-телекоммуникационных системах (ИТКС), согласно [1], следует понимать совокупность мероприятий, направленных на выявление угроз государственным ИР от осуществления несанкционированных действий в ИТКС. Согласно [1], объектом оценивания защищенности является состояние защищенности государственных ИР, которые обрабатываются в ИТКС, независимо от наличия комплексной системы защиты информации (КСЗИ), которая осуществляется с целью выявления существующих угроз государственным ИР в ИТКС и является составной частью мер по защите информации. Ответственность за проведение оценивания защищенности возлагается на Государственную службу специальной связи и защиты информации Украины (Госспецсвязь). Одной из задач Госспецсвязи, в соответствии с [1], является разработка общей программы и методики оценивания защищенности в органах государственной власти, органах местного самоуправления, воинских формированиях, предприятиях, учреждениях и организациях независимо от форм собственности, а также отдельные программы и методики оценивания защищенности зависимо от вида ИТКС и режима доступа к информации, которая в них обрабатывается. Кроме этого, в Концепции создания государственной системы защиты критической инфраструктуры Украины от 2017 г. [2] указано отсутствие единой методологии проведения оценивания угроз критической инфраструктуре.

Опыт Грузии

Рассматривая законодательную базу Грузии, важно отметить, что в 2010 г. было создано Агентство по обмену данными (DEA) при Министерстве юстиции Грузии [3]. В компетенцию DEA входит обеспечение кибербезопасности всей правительственной сети (за исключением ее военной части). DEA устанавливает минимальные требования по информационной безопасности для критических информационных систем. Под руководством DEA функционирует Компьютерная группа реагирования на чрезвычайные ситуации (CERT) – она отвечает за реагирование на киберинциденты и наблюдение за работоспособностью правительственной сети Грузии. CERT уполномочена требовать доступ к критическим информационным системам или активам. На международном уровне Грузия в 2012 г. ратифицировала Конвенцию о киберпреступности, разработанную Советом Европы. В 2015 г. был принят Закон Грузии «О порядке планирования и координации политики национальной безопасности», где сфера информационной безопасности (статья 11) включает действия по обеспечение защиты критических информационных систем [4]. Кроме того, в январе 2017 г. была принята национальная Стратегия по кибербезопасности и план действий на 2017-2018 гг., где одной из задач является исследование критериев идентификации и стандартов для КИИ [5]. Анализируя ситуацию в Грузии, можно сделать вывод, что страна поддерживает политику

Европейского Союза (ЕС) в области кибербезопасности, но, так же как и Украина, будучи ассоциированным членом ЕС, на данный момент не сформировано список объектов КИИ и, соответственно, методов и методик по их защите.

Опыт США

В январе 2014 г. в США был создан National Critical Information Infrastructure Protection Centre (NCIIPC), главной целью которого является оценивания уровня кибербезопасности в КИИ. Позже был разработан специальный документ – NCIIPC Framework for Evaluating Cyber Security in Critical Information Infrastructure [6] в котором предложен алгоритм оценивания кибербезопасности в КИИ (Рис. 2). Этот Framework демонстрирует 5 этапов проведения оценивания уровня кибербезопасности КИИ и показывает роль NCIIP в этом процессе. Однако, эта структура является вспомогательным механизмом, направленным на то, чтобы дать представление о процессе оценивания уровня кибербезопасности в рамках определенной организации, а не отрасли.

Опыт РФ

Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий разработало «Методические рекомендации по оценке защищенности критически важных объектов» (Рекомендации РФ) [7]. В Рекомендациях РФ оценивается состояние защиты критически важных объектов по уровню реализации мероприятий повышения их защищенности. В Рекомендациях РФ под защищённостью объекта понимается состояние (способность), при котором предотвращаются, преодолеваются или предельно снижаются негативные последствия возникновения потенциальных опасностей от угроз техногенного, природного характера и террористических проявлений. Однако, в Рекомендациях РФ под защитой критически важных объектов понимают только физическое или инженерно-техническая защита. Это обусловлено тем, что ИР и информационная система не считается критически важным объектом.

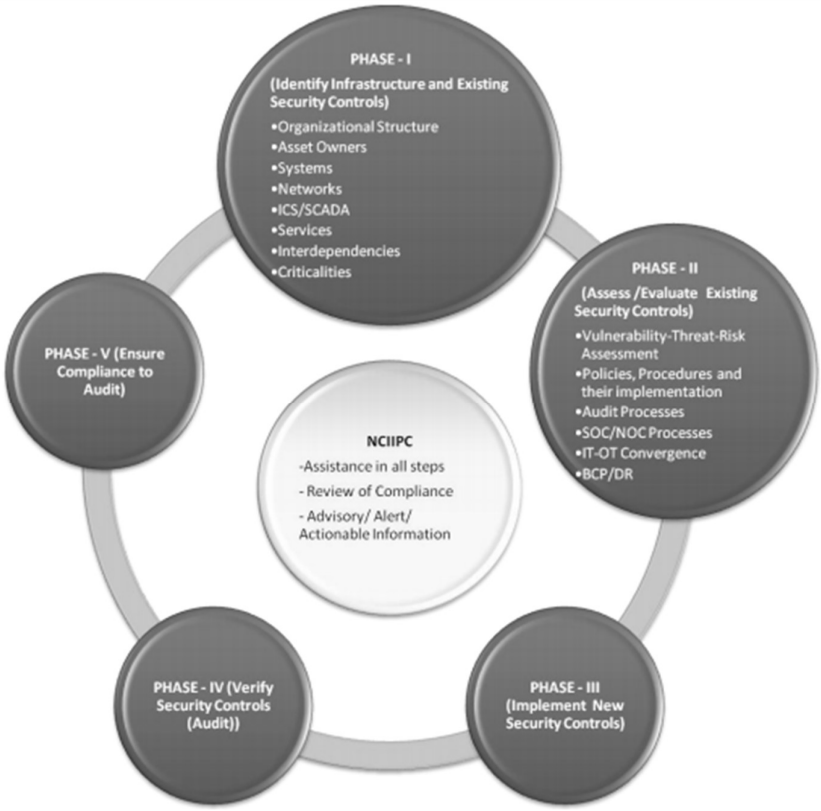

Рис. 2. Схема оценивания кибербезопасности в КИИ [4]

Результаты научных исследований в области защиты КИИ

Невойт Я.В. в диссертационной работе [8] разработала метод оценивания защищенности ИР на основе исследования источников угроз информационной безопасности. В работе были решены следующие задачи: по совокупности наиболее опасных угроз, на которые должны быть направлены первоочередные меры защиты, – сформировано совокупности пар «угроза-уязвимость»; по совокупности сложившихся пар «угроза-уязвимость» – определяется индекс защищенности ИР и вычисляется комплексный показатель их защищенности. Однако, в данном методе используется не полный перечень угроз и уязвимостей, что не позволяет эффективно повысить уровень обеспечения информационной безопасности.

Янчук В.А. разработал методику оценивания защиты информационных локальных объектов системы электронного управления [9]. Исследователь определяет эффективность защищенности информации локальных объектов системы электронного управления через эффективность комплекса мер по защите информации локальных объектов системы электронного управления и оценивает степень защищенности информации локальных объектов системы электронного управления. Однако, автор не адаптировал указанную методику для оценки эффективности защиты информации в информационной системе в обобщенном случае, например, для оценки эффективности состояния защиты информации объекта -сфера-отрасль общественной деятельности государства, а также для оценивания состояния защиты информации в государстве.

Бурькова Е.В. исследовала задачи оценивания защищенности информационных систем персональных данных [10]. Автором была разработана схема этапов оценки защищенности персональных данных в информационных системах, однако в этой работе

большее внимание уделяется защите самой информационной системы, а не ИР; а также не исследуются основные характеристики информации.

В работе Евсеева С.П. предложена методология оценивания безопасности информационно-коммуникационных технологий на примере автоматизированных банковских систем, которая базируется на концепции стратегического управления безопасностью указанных систем [11]. Предлагаемая концепция предполагает синергетический подход к выбору наиболее эффективных направлений достижения поставленных целей кибербезопасности с учетом величины риска на каждом уровне модели стратегического управления. Подобный выбор позволяет комплексно проводить отбор альтернативных вариантов возможных стратегических решений по вопросам кибербезопасности. Однако, предложенная концепция ориентирована исключительно на банковский сектор, не является универсальной и не может применяться для других отраслей КИИ.

Голобородько М.Ю., Курченко А.А. и Кирис А.С разработали метод числовой оценки уровня защищенности информации в сегменте корпоративной информационной системы [12]. В исследовании использован вероятностно-статический подход, при котором не учитывается динамика изменения значений вероятность угроз и уязвимости информации во времени. Оцениваются также априорные ожидаемые значения вероятности нарушения защищенности информации. Однако, для получения информации, необходимой для расчета приведенных показателей метода, обязательным условием является наличие системы мониторинга деятельности информационной службы предприятия.

Сидоренко В.Н. разработала метод оценки уровня кибербезопасности [13], который дает возможность рассчитать количественные параметры, характеризующие защищенность определенной области или КИИ государства в целом. Однако, в данной работе, при разработке методики не принимались во внимания характеристики информации и влияния человеческого фактора на ситуацию.

Исследователями Soon-Tai Park, Jong-Whoi Shin, Bog-Ki Min, Ik-Sub Lee, Gang-Shin Lee и Jae-Il Lee была предложена методика оценивания уровня информационной безопасности объектов КИИ [14], которая включает процедуры для измерения уровня безопасности организации и получение уровня зрелости путем анализа данных. Авторами были созданы контрольные списки для 12 категорий управления, которые будут оцениваться на пяти уровнях. На основе модели измерения зрелости SSE-CMM и SP800-26, предлагаемые пять уровней были разработаны в качестве контрольных. Далее сертифицированными аудиторами проводится заполнения контрольных листов и выставления оценки по 12 категориям. Как только результаты оценки будут подтверждены, оценки для каждого элемента управления рассчитываются для оценки уровня информационной безопасности организации. Однако, данная методика не учитывает специфику отраслей КИИ и есть базовым аудитом уровня информационной безопасности предприятия.

В табл. 1 отображены результаты анализа подходов и методов оценивания защищённости ИР в объектах КИИ по таким критериям: SS – учет способов и средств кибербезопасности; ICT – учет имплементации ИКТ; QP – вывод количественных показателей; CIIP – оценивание отраслей КИИ; UN – универсальность; HF – учет человеческого фактора при оценке; IP – учет характеристик безопасности информации (основных и дополнительных).

Подходы и методы оценивания
защищённости ИР в объектах КИИ

Таблица 1

Критерии / Название метода	SS	ICT	QP	CIIP	UN	HF	IP
NCIIPC Framework	+	+	-	-	+	+	-
Рекомендации РФ	+	+	+	+	-	+	-
Невойт Я.В.	-	-	+	-	+	+	-
Янчук В.А.	-	+	+	+	-	-	-
Бурькова Е.В.	-	+	-	-	+	-	-
Евсеев С.П.	+	+	+	-	-		
Голобородько М.Ю., Курченко А.А., Кирис А.С	+	+	+	-	+	+	-
Сидоренко В.Н.	+	+	+	+	+	-	-
Soon-Tai Park, Jong-Whoi Shin et al	-	+	+	-	+	+	-

Выводы

Таким образом, в данной работе проведен многокритериальный анализ подходов и методов оценивания защищённости ИР в объектах КИИ. Установлено, что на сегодня не разработан универсальный метод оценивания, который учитывает все критерии для качественного оценивания защищённости ИР объектов КИИ. В дальнейших исследованиях, с учетом результатов этой работы, планируется разработать метод оценивания, который будет учитывать особенности информационной составляющей и позволит оценить защищённости ИР объектов КИИ.

БИБЛИОГРАФИЯ

1. Наказ 04.07.2008 N 112 Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. URL: http://za kon. rada.gov.ua/laws/show/z0690-08.

2. Розпорядження від 6 грудня 2017 р. № 1009-р Про схвалення Концепції створення державної системи захисту критичної інфраструктури. URL: http://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80.

3. Закон Грузии Об информационной безопасности от 5 июня 2012 года №6391-Ic. URL: https://matsne.gov.ge/en/document/download/1679424/3/ru/pdf.

4. Закон Грузии О порядке планирования и координации политики национальной безопасности. URL: https://matsne.gov.ge/en/document/download/2764463/2/ru/pdf.

5. Cybersecurity Strategy of Georgia 2017 -2018. URL: http://csbd. gov.ge/doc /Cybersecurity%20Strategy_eng.pdf.

6. NCIIPC Framework for Evaluating Cyber Security in Critical Information Infrastructure, version 1. URL: http://nciipc.gov.in/documents/Evaluating_ Cyber_ Security_Framework.pdf.

7. Методические рекомендации по разработке планов повышения защищенности критически важных объектов, территорий субъектов Российской Федерации и муниципальных образований (утв. МЧС России 28 декабря 2011 г. N 2-4-60-21-14). URL: http://base.garant.ru/71408274/.

8. Невойт Я.В. «Метод оцінювання стану захищеності інформаційних ресурсів на основі дослідження джерел загроз інформаційній безпеці»: дис. канд. техн. наук. ДУТ, Київ, 2016. URL: http://www.dut.edu.ua/uloads/ p_1539_26349739.pdf.

9. Янчук В.О «Методика оцінювання стану захисту інформації локальних об'єктів системи електронного врядування». URL: http://academy. gov.ua/ej/ej11/txts/10ivoseu.pdf.

10. Бурькова Е.В. «Задача оценки защищенности информационных систем персональных данных». *Вестник Чувашского университета*. 2016. № 1. С. 112–118.

11. Евсеев С. П. «Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины». *Безпека інформації*. 2016. Т. 22, № 3. С. 297-309.

12. Голобородько М.Ю, Курченко О.А., Кирись О.С. «Методи числової оцінки рівня захищеності інформації у сегменті корпоративної інформаційної системи». *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*, №2(51), 2014р. С. 137-139.

13. В. Сидоренко, А. Положенцев, С. Гнатюк, «Метод оцінювання рівня кібербезпеки галузі критичної інформаційної інфраструктури держави», *Вісник інженерної академії України*, вип. 4, с. 142-148, 2017.

14. Soon-Tai Park, Jong-Whoi Shin, Bog-Ki Min, Ik-Sub Lee, Gang-Shin Lee and Jae-Il Lee, « Evaluation Method for Information Security Levels of CIIP (Critical Information Infrastructure Protection)», *World Academy of Science, Engineering and Technology International Journal of Information and Communication Engineering,* Vol:2, No:2, 2008, p.446-449.