Система информационной безопасности экосистемы цифровых платежей: оптимизация мер защиты

А. В. Олифиров, К. А. Маковейчук, Н. И. Потапович

***Аннотация* — В статье предложен инкрементальный подход к оптимизации мер защиты цифровых платежных экосистем. Установлено, что основой развития национальных экономик являются информационные и цифровые технологии, система распределенного реестра и платформенные решения, которые формируют новые технологические экосистемы. Показано, что в современных условиях платежные экосистемы трансформируются для работы с цифровыми национальными валютами. Отмечено, что главной проблемой реализации концепции цифровой валюты центрального банка является обеспечение информационной безопасности ее экосистемы. Определена целевая модель создания и использования платежной экосистемы цифровой валюты центрального банка. Предложена модель платежной экосистемы на основе платежного шаблона транзакций. Показано, что в результате декомпозиции на основе инкрементального подхода можно определить угрозы и меры защиты по каждому подшаблону и каждому целевому классу платежной экосистемы цифровой валюты центрального банка, то есть можно исследовать как можно напасть на каждый элемент и на сервис платежной экосистемы CBDC и как эту атаку можно отвести и ослабить. Построена экономико-математическая модель для оптимизации полученного полного набора мер защиты цифровой платежной экосистемы.**

***Ключевые слова* — Инкрементальный анализ, информационная безопасность, меры защиты платежей, цифровая валюта центрального банка, цифровая платежная экосистема, цифровые технологии, экономико-математическая модель.**

I. ВВЕДЕНИЕ

В условиях финансовой нестабильности, обусловленной внешними вызовами, развитием финансовых технологий и использованием криптовалют, вопросы обеспечения информационной безопасности цифровой платежной системы представляют определенный теоретический и практический интерес [1-4].

Цифровая экономика основывается на беспроводных технологиях, искусственном интеллекте, технологиях виртуальной и дополненной реальности, системе распределенного реестра и платформенных решениях, которые формируют технологические экосистемы. Экономика в России переходит на платформенные модели и экосистемы в различных сферах деятельности. В Росси финансовый сектор занимает лидирующая роль в создании экосистем. Технологические экосистемы сформировались и в сфере электронных платежей [5-10].

Цифровая платежная экосистема представляет собой технологии, методы и договоренностей, позволяющая оказывать сервис по расчетам между контрагентами в сети Интернет и в других сетях передачи данных [5,6]. Появление крупнейших мировых экосистем на базе больших технологических компаний, обладающих широкой клиентской базой криптовалют вынуждает центробанки обратиться к концепции цифровой валюты центрального банка (CBDC) [11-14]. В настоящее время многие страны реализуют пилотные проекты по переходу на цифровую национальную валюту. Эти проекты нацелены на контроль цифровой валюты со стороны государства, позволяют снизить транзакционные расходы и предоставляют много других преимуществ, но, вместе с тем, реализация этих проектов несет много рисков, которыми необходимо управлять, применять соответствующие меры защиты [15-22]. В связи с этим, представляется актуальным исследование системы информационной безопасности цифровой платежной экосистемы в части оптимизации мер защиты.

Методология данной работы включает следующее:

– сбор данных и научное обобщение публикаций по информационной безопасности платежных систем, что позволяет уточнить понятийный аппарат в сфере электронных платежей;
– экосистемный подход к объекту исследования, суть которого состоит в том, что адаптировать свои традиционные платежные системы под возможности и вызовы возникающих технологических экосистем;
– инкрементальный анализ, который позволяет выполнять реализацию проекта постепенно,

Статья получена 11 ноября 2024. .

Статья подготовлена по результатам исследований, выполненных при поддержке гранта РНФ (№ 24-28-20431).

Александр Васильевич Олифиров, доктор экономических наук, профессор, профессор кафедры экономики и финансов, Гуманитарно-педагогическая академия (филиал) ФГАОУ ВО "Крымский федеральный университет им. В. И. Вернадского" в г. Ялте (e-mail: alex.olifirov@gmail.com)

Кристина Александровна Маковейчук, кандидат экономических наук, доцент, доцент кафедры искусственного интеллекта, ФГБОУ ВО "Финансовый университет при Правительстве Российской Федерации", г. Москва (e-mail: christin2003@yandex.ru)

Никита Игоревич Потапович, магистрант кафедры экономики и финансов, Гуманитарно-педагогическая академия (филиал) ФГАОУ ВО "Крымский федеральный университет им. В. И. Вернадского" в г. Ялте (e-mail: n.potapovich@mail.ru)

частично интегрируя новый функционал в уже существующую экосистему CBDC, при этом весь проект перехода на цифровую платежную экосистему разбивается на небольшие части, которые можно быстро разрабатывать и тестировать отдельно от других;

– применение экономико-математических методов для оптимизации состава мер защиты платежей в цифровой платежной экосистеме.

Цель данной работы – определить состав и оптимизировать меры защиты цифровой платежной экосистемы в условиях перехода на цифровую валюту центрального банка.

II. ЦЕЛЕВАЯ МОДЕЛЬ СОЗДАНИЯ И ИСПОЛЬЗОВАНИЯ ЭКОСИСТЕМЫ ЦИФРОВОЙ ВАЛЮТЫ ЦЕНТРАЛЬНОГО БАНКА

Определим токены как цифровые активы, которые представляют собой какую-либо ценность и выпускаются на базе блокчейна. Как и криптовалюта, CDBC – это цифровой токен, привязанный к стоимости фиатной валюты этой страны. Токены CBDC выпускаются Центральным банком. Следует отметить CBDC контролируется, регулируется и выпускается монетарными властями страны, в которой находится цифровая валюта этого Центрального банка [23-24].

Целевая модель создания и использования экосистемы цифровой валюты центрального банка представлена в таблице I.

Платежная (цифровая) экосистема CBDC – совокупность сервисов, в том числе платформенных решений, одной группы компаний, позволяющих пользователям получать широкий круг платежных услуг в рамках единого бесшовного интегрированного процесса [5-6].

При выборе модели для создания прототипа платформы CDBC в результате анализа информации о практическом опыте ряда центральных банков, наиболее предпочтительной оказалась гибридная модель, которая включает как компоненты централизованной системы, так и распределенных реестров и объединяет централизованный и децентрализованный подходы. При реализации этой модели центральный банк открывает и ведет кошельки банкам (финансовым посредникам).Далее банки открывают и ведут кошельки клиентов и предоставляют им мобильные приложения для проведения расчетов и осуществляют расчеты по их поручению (рисунок 1) [7-8].

Таблица I: Целевая модель создания и использования экосистемы цифровой валюты центрального банка

Этап создания и использования экосистемы	Субъект экосистемы	Цели экосистемы цифровой валюты центрального банка
Этап 1. Поставка технологий экосистемы CBDC	Поставщик технологий	Создать платформу для расчетов в CBDC.
Этап 2. Эмиссия цифровой валюты	Эмитент	Осуществить эмиссию цифровой валюты
Этап 3. Поставка учетных записей	Поставщик учетных записей	Обеспечить пользователям возможность регистрироваться, получать платежные учетные данные (в форме цифрового кошелька) и совершать платежи CBDC.
Этап 4. Транзакция для покупки товаров за CBDC	Отправитель платежа (покупатель), получатель платежа (продавец), валидатор	Обеспечить транзакцию, возможность покупателю через мобильное приложение банка подтвердить оплату со своего кошелька. Обеспечить возможность перевода CBDC с кошелька покупателя на кошелек продавца, возможность утверждения платежа, занесения учетных записей в хранилище данных, в базу данных или в реестр или в модель токена.

Выполнение платежа, представленного на рисунке 1, реализуется через мобильное приложение банка с подтверждением перевода с кошелька покупателя на кошелек продавца с занесением учетных записей в хранилище данных, в базу данных или в реестр, или в модель токена следующими операциями:

1 – Участник 1 дает поручение Банку 1 на перевод CDBC со своего кошелька на кошелек Участника 2;

2 – Банк 1 переводит CDBC с кошелька Участника 1 на кошелек Участника 2;

3 – Банк 2 зачисляет CDBC на кошелек Участника 2;

4 – Банк 2 сообщает Участнику 2 о поступлении CDBC на его кошелек;

5 – Банк 2 информирует Банк 1 о поступлении CDBC на кошелек Участник 2.

Экосистема CBDC создается на основе построения цифровой платформы для расчетов и осуществления эмиссии цифровой валюты, обеспечения пользователей возможностью регистрироваться, получать платежные учетные данные (в форме цифрового кошелька) и совершать платежи [11].

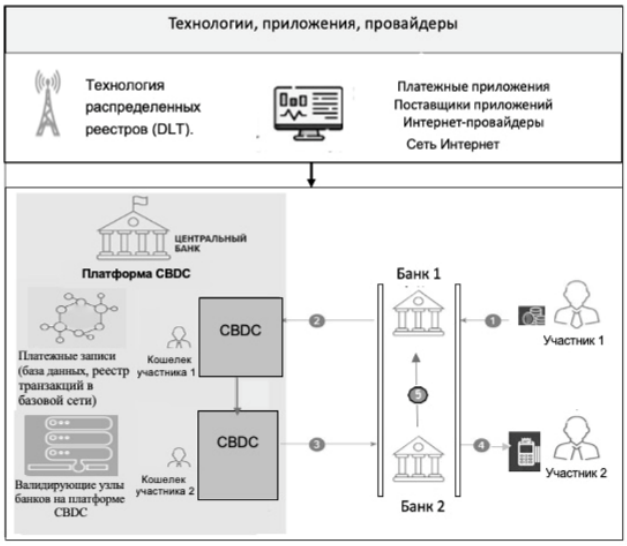

Рис. 1: Технологические аспекты реализации прототипа экосистемы цифровой валюты центрального банка на основе компонентов централизованной системы и технологии распределенных реестров

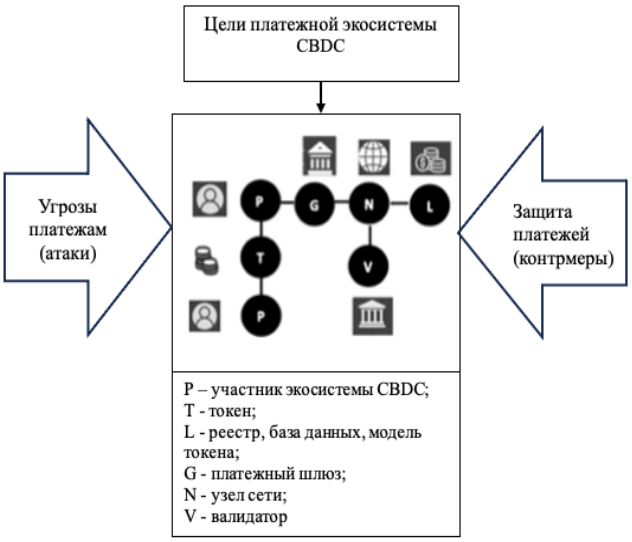

Рис. 2: Модель платежной экосистемы CBDC на основе платежного шаблона транзакции

III. МОДЕЛЬ ПЛАТЕЖНОЙ ЭКОСИСТЕМЫ CBDC И ЕЕ ДЕКОМПОЗИЦИЯ

Рассмотрим инкрементальный анализ, который позволяет выполнять реализацию проекта перехода на цифровую валюту центрального банка постепенно, частично интегрируя новый функционал в уже существующую экосистему CBDC на основе использования шаблонов и подшаблонов. Этот подход с позиций оценки информационной безопасности имеет ряд преимуществ. Он позволяет добавлять новые функции постепенно, что значительно ускоряет процесс разработки и улучшает качества продукта, позволяет тестировать каждый новый компонент системы отдельно, что уменьшает количество ошибок и повышает качество финального продукта. Главная идея этого подхода заключается в том, что вместо того, чтобы разрабатывать и тестировать продукт целиком, весь проект разбивается на небольшие части, которые можно быстро разрабатывать и тестировать отдельно от других [25-26].

Модель платежной экосистемы CBDC на основе платежного шаблона транзакции представлена на рисунке 2.

Эта модель платежной экосистемы CBDC на основе платежного шаблона транзакции работает по следующему алгоритму [5,6].

1. При оплате – токен (идентификационный код) покупателем передается продавцу (P-T-P).

2. Продавец (мерчант) передает токен своему торговому эквайеру, торговый эквайер (поставщик услуги эквайринга) передает токен через шлюз в сеть (P-G-N).

3. После передачи в сеть данные поступают в реестр транзакций, или базу данных или модель токена (банковское хранилище) (N-L).

4. Сеть обращается к своему "хранилищу", чтобы сопоставить токен с данными покупателя (L-N).

5. Сеть передает токен и другие данные в банк (валидатору) на утверждение (N-V).

6. Валидатор проверяет средства и авторизует транзакцию, авторизация передается в сеть (V-N), и возвращается к торговому эквайеру, продавцу и покупателю по сети (N-G-P).

Далее в рамках инкрементального анализа, платежный шаблон в экосистеме CBDC разобьем на подшаблоны (рисунок 3).

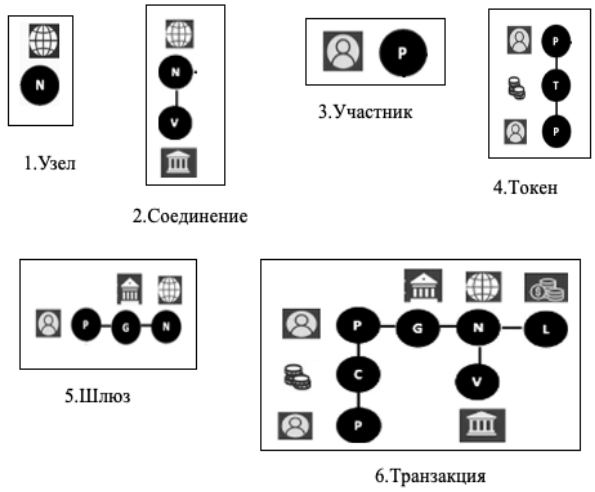

Рис. 3: Подшаблоны платежной экосистемы цифровой валюты центрального банка

Процесс декомпозиции должен быть последовательным и постепенным и должен включать элементы, объединение которых позволит сформировать полный шаблона.

Процесс начинается с самого маленького строительного шаблона, в данном случае узла, называемого подшаблоном «Узел». Второй подшаблон «Соединение» добавляется к первому. Каждый подшаблон с каждым разом формирует более полный шаблон. Таким образом, более сложные шаблоны создаются из менее сложных компонентов, которые уже

завершили анализ угроз и мер защиты. Такой подход позволяет один раз завершить набор конструкций исходных подшаблонов и использовать их повторно.

Далее в рамках инкрементального анализа, цели платежной системы разделим на цели подшаблонов (цели узла, соединения, участника, токена, шлюза, транзакции) и цели целевых классов платежной системы (цели приложения, сервиса, протокола, сети, данных, физического окружения). Тогда представленная на рисунке 2 структура "Цели-Угрозы -Защита" может быть детализирована так, как это показано в таблице II.

Далее в таблице III осуществляем детальную декомпозиция целей подшаблонов платежной экосистемы CBDC по целевым классам.

Таблица II: Цели, угрозы и защита (контрмеры) платежной экосистемы CBDC по целевым классам внутри каждого подшаблона

Цели подшаблонов платежной экосистемы CBDC	Цели платежной экосистемы CBDC (по целевым классам)	Угрозы экосистеме платежей CBDC	Защита (контрмеры)
1. Цели узла 2. Цели соединения (TCP-соединения, дающего 2 узла и соединение) 3. Цели участника (покупателя, продавца, торгового эквайера) 4. Цели токена (передача, трансфер токена) 5. Цели шлюза (платежного шлюза, провайдера) 6. Цели транзакции: (покупки физических товаров в цифровой валюте центрального банка)	1. Цели приложения 2. Цели сервиса 3. Цели протокола 4. Цели сети 5. Цели данных 6. Физические цели	1. Угрозы приложению 2. Угрозы сервису 3. Угрозы протоколу 4. Угрозы сети 5. Угрозы данным 6. Угрозы физическим объектам	1. Защита приложения 2. Защита сервиса 3. Защита протокола 4. Защита сети 5. Защита данных 6. Защита физических объектов

Таблица III: Декомпозиция целей подшаблонов платежной экосистемы CBDC по целевым классам

Цели подшаблонов экосистемы платежей CBDC	Цели платежной экосистемы CBDC (по целевым классам)					
	1. Цели приложения	2. Цели сервиса	3. Цели протокола	4. Цели сети	5. Цели данных	6. Цели физических объектов
1. Цели узла				Таблица IP-маршрутизации Сетевое устройство	IP-адрес	Операционная зона узла
2. Цели соединения	Децентрализованная координация	TCP-соединение	P2P-сеть			
3. Цели участника	Кошелек / Браузер		Участник / Кошелек / Устройство	Интерфейсное устройство участника	Идентификация Учетная запись Закрытый ключ	Участник
4. Цели токена	P2P-передача токена Цифровой актив - токен	Метка времени	Протокол передачи токенов		Данные передачи токена Данные журнала сеанса	
5. Цели шлюза		Интерфейс /сессия	Участник / Кошелек / Платежный шлюз		Идентификация платежного шлюза	
6. Цели транзакции	P2P DC-платёж	Сервис DC-транзакций	Участник / Кошелек / Шлюз / Платеж		Данные транзакции	

IV. ФОРМИРОВАНИЕ МЕР ЗАЩИТЫ ПЛАТЕЖНОЙ ЭКОСИСТЕМЫ CBDC И ИХ ОПТИМИЗАЦИЯ

Затем в результате дальнейшей декомпозиции можно сформировать меры защиты по каждому подшаблону и каждому целевому классу, как это показано в таблице IV на примере подшаблона «Узел».

Так могут быть представлены все меры защиты платежной экосистемы по всем целевым классам. Для каждой цели подшаблона и для каждого класса цели

можно исследовать ситуацию относительно того, как можно напасть на сервис (элемент) платежной экосистемы CBDC и как эту атаку можно отклонить и ослабить.

Таблица IV: Формирование мер защиты по подшаблону «Узел» в целевом классе «Таблица IP-маршрутизации»

Цели подшаблонов платежной экосистемы CBDC	Цели платежной экосистемы CBDC (по целевым классам)	Угрозы платежной экосистеме CBDC	Защита (контрмеры) платежной экосистемы CBDC
1. Цели узла	Цели сети: Таблица IP-маршрутизации	Угрозы атаки на таблицу маршрутизации узлов системы заключаются в повреждении данных IP-адресов в таблице маршрутизации, которая включает сетевой адрес, сетевую маску, адрес маршрутизатора, интерфейс и метрику. Повреждения осуществляются путем отправки "бесполезных" данных в формате IP во входящие TCP-соединения. А также путем непосредственной злонамеренной фальсификации данных таблицы маршрутизации.	1. Увеличение размера списка адресов. 2. Увеличение частоты обновления. 3. Выбор IP-адреса с долгоживущим соединением. 4. Ограничение нежелательных сообщений. 5. Регулярный мониторинг активности канала. 6. Ограниченный доступ в операционную зону узла (системы видеонаблюдения и сигнализации).

В итоге получаем полный набор мер защиты, которые можно оптимизировать с помощью модели целочисленного линейного программирования [27, 28].

Эта модель позволяет выбрать состав мер защиты информационной безопасности (ИБ) при минимизации остаточного риска и при установленных ограничениях затрат на меры защиты системы информационной безопасности.

В данной постановке задачи определяются целочисленные переменные x_j, которые минимизируют функцию:

$$F = \sum_{i=1}^{m} VLR_i - \sum_{j=1}^{n} a_{ij} * x_j \to min, \quad (1)$$

при следующих ограничениях:

$$\sum_{j=1}^{n} c_j * x_j \leq s, \quad (2)$$

$$x_j \in \{0; 1\}, j = \overline{1, n}, \quad (3)$$

где x_j - целочисленная булева переменная, которая равна:

$$x_j = \begin{cases} 1, \text{если } j - \text{тая мера ИБ используется} \\ \text{для противодействия угрозам} \\ 0, \text{в противном случае} \end{cases};$$

VLR_i – риск ИБ по i-той угрозе, присущий системе без использования мер ИБ;

a_{ij} - риск, отведенный j-той контрмерой по i-той угрозе;

c_j – стоимость реализации j-той контрмеры ИБ;

s – допустимый размер затрат на обеспечение мер ИБ.

Таким образом, целевая функция (1) минимизирует остаточный риск ИБ в системе CBDC. Ограничение (2) указывает на то, что затраты на меры ИБ не могут превышать s. Ограничение (3) отражает целочисленность модели.

V. Заключение

Исследование многих работ по экосистемам CBDC сосредоточено на дизайне валют, на распределенном реестре или модели токенов, в то время как главной проблемой реализации концепции системы цифровой валюты центрального банка является обеспечение ее информационной безопасности.

Предложен подход к оптимизации мер защиты информационной безопасности платежной экосистемы CBDC, с использованием модели экосистемы CBDC на основе платежного шаблона. Этот подход, в соответствии с методологией инкрементного анализа, позволяет сформировать меры защиты по каждому подшаблону и каждому целевому классу экосистемы CBDC и получить полный набор мер защиты цифровой платежной экосистемы. Выбрать оптимальный набор мер защиты информационной безопасности позволяет модель целочисленного линейного программирования.

Библиография

[1] Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.

[2] Милославская Н.Г., Толстой А.И. Управление информационной безопасностью. М.: НИЯУ МИФИ, 2020. – 536 с.

[3] Olifirov A., Makoveichuk K., Petrenko S. Cybersecurity measures of the digital payment ecosystem. In Selected Papers of 11th International Scientific and Technical Conference on Secure Information Technologies (BIT 2021). CEUR Workshop Proceedings, 2021, Vol-3035, pp. 133-142.

[4] Brantly, A. F. Risk and uncertainty can be analyzed in cyberspace, Journal of Cybersecurity, volume 7, issue 1, 2021, tyab001. DOI: 10.1093/cybsec/tyab001.

[5] Yu, H., Hsi, K., & Kuo, P. (2002). Electronic payment systems: an analysis and comparison of types. Technology in Society, 24, pp. 331-347. DOI: 10.1016/S0160-791X(02)00012-X.

[6] Raharja, S. U. J., Muhyi, H. A., Herawaty, T. Digital payment as an enabler for business opportunities: A go-pay case study. Review of Integrative Business and Economics Research, 9(1) (2020), pp. 319-329. URL: http://buscompress.com/uploads/3/4/9/8/34980536/riber_9-s1_25_b19-102_319-329.pdf.

[7] Staykova, Kalina & Damsgaard, Jan. (2016). Adoption of Mobile Payment Platforms: Managing Reach and Range. Journal of theoretical and applied electronic commerce research, 11(3), pp. 66-85. DOI: 10.4067/S0718-18762016000300006.

[8] Экосистемы: подходы к регулированию. Доклад для общественных консультаций, Москва, 2021. https://www.cbr.ru/Content/Document/File/119960/Consultation_Paper_02042021.pdf.

[9] Хоменко Е. Г. Электронные платежные системы в России и в зарубежных странах. Актуальные проблемы российского права. 2019; (8): 159-164. https://doi.org/10.17803/1994-1471.2019.105.8.159-164.

[10] Lin, W. R., Lin, C. -Y., & Ding, Y. -H. (2020). Factors Affecting the Behavioral Intention to Adopt Mobile Payment: An Empirical Study in Taiwan. Mathematics, 8(10), 1851. https://doi.org/10.3390/math8101851.

[11] "Концепция цифрового рубля" (подготовлена Банком России). – URL: http://www.consultant.ru/document/cons_doc_LAW_381918/ (дата обращения: 01.09.2021).

[12] Масленников В. В., Ларионов А. В. Цифровые валюты: концептуализация рисков и возможности регулирования. Мир новой экономики. 2021, 15(4):16-28. https://doi.org/10.26794/2220-6469-2021-15-4-16-28

[13] Agur I., Lavayssière X., Bauer G. V., Deodoro J., Peria S. M., Sandri D., Tourpe H. Lessons from crypto assets for the design of energy efficient digital currencies. Ecological Economics, 2023, Vol-212. https://doi.org/10.1016/j.ecolecon.2023.107888.

[14] Gilbert S., Loi H. Digital Currency Risk. International Journal of Economics and Finance, 2018, Vol-10, No. 2. DOI: 10.5539/ijef.v10n2p108.

[15] Olifirov A.V., Makoveichuk K.A., Petrenko S.A. Integration of cyber security into the Smart Grid operational risk management system. In Selected Papers of the 4th All-Russian Scientific and Practical Conference with International Participation "Information Systems and Technologies in Modeling and Control" (ISTMC 2019). CEUR Workshop Proceedings, 2019, Vol-2522, pp. 132-144. URL: https://ceur-ws.org/Vol-2522/paper14.pdf.

[16] Petrenko, A. A., Petrenko, S. A., Makoveichuk, K. A., Olifirov, A. V. Methodological recommendations for the cyber risks management, CEUR Workshop Proceedings, 2021, Vol-2914, pp. 234-247. URL: http://ceur-ws.org/Vol-2914/paper20.pdf.

[17] Petrenko, S., Petrenko, A., Makoveichuk, K.A., Olifirov, A. (2021). Development of a Cyber-Resistant Platform for the Internet of Things Based on Dynamic Control Technology. In: Singh, P.K., Veselov, G., Vyatkin, V., Pljonkin, A., Dodero, J.M., Kumar, Y. (eds) Futuristic Trends in Network and Communication Technologies. FTNCT 2020. Communications in Computer and Information Science, vol 1395. Springer, Singapore. https://doi.org/10.1007/978-981-16-1480-4_13.

[18] Petrenko, S. A., Makoveichuk, K. A., Olifirov, A. V. Concept of cyber immunity of industry 4.0. CEUR Workshop Proceedings, 2019, Vol-2603, pp. 93-99. URL: http://ceur-ws.org/Vol2603/paper20.pdf.

[19] Petrenko, S., Makoveichuk, K., Olifirov, A. (2020). New Methods of the Cybersecurity Knowledge Management Analytics. In: Sukhomlin, V., Zubareva, E. (eds) Convergent Cognitive Information Technologies. Convergent 2018. Communications in Computer and Information Science, vol 1140. Springer, Cham. https://doi.org/10.1007/978-3-030-37436-5_27.

[20] Банк России. Основные типы компьютерных атак в кредитно-финансовой сфере в 2019–2020 годах. Москва, 2021, URL: https://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf.

[21] Boholm, M. Twenty-five years of cyber threats in the news: a study of Swedish newspaper coverage (1995–2019), Journal of Cybersecurity, Volume 7, Issue 1, 2021, tyab016, https://doi.org/10.1093/cybsec/tyab016.

[22] Agrafiotis. I., Nurse, J. R. C., Goldsmith M., Creese, S., Upton, D, A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, Journal of Cybersecurity, Volume 4, Issue 1, 2018, tyy006, https://doi.org/10.1093/cybsec/tyy006.

[23] Янковский Р. М. Криптовалюты в российском праве: суррогаты, "иное имущество" и цифровые деньги // Право. Журнал Высшей школы экономики. 2020. № 4. URL: https://cyberleninka.ru/article/n/kriptovalyuty-v-rossiyskom-prave-surrogaty-inoe-imuschestvo-i-tsifrovye-dengi.

[24] Бауэр В.П., Смирнов В.В. Институциональные особенности разработки конкурентоспособной криптовалюты. Финансы: теория и практика/Finance: Theory and Practice. 2020;24(5):84-99. https://doi.org/10.26794/2587-5671-2020-24-5-84-99.

[25] Courtier, P., Thépaut, J.-N., Hollingsworth, A. A strategy for operational implementation of 4D-Var, using an incremental approach. Quarterly Journal of the Royal Meteorological Society, 1994, Vol-120, Issue 519, pp. 1367-1387. https://doi.org/10.1002/qj.49712051912.

[26] Sun, P., Li, X., & Ting, M. Y. Efficient incremental analysis of on-chip power grid via sparse approximation. In Proceedings - Design Automation Conference, 2011, pp. 676–681. https://doi.org/10.1145/2024724.2024878.

[27] Олифиров, А. В. Модели управления рисками экономических информационных систем / А. В. Олифиров // Информационные системы и технологии в моделировании и управлении : Материалы всероссийской научно-практической конференции, Ялта, 05–07 июля 2017 года / Ответственных редактор Н.Н. Олейников. – Ялта: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2017. – С. 465-470. – EDN YYVSVL.

[28] Олифиров, А. В. Организационно-технические меры информационной безопасности цифровой валюты центрального банка / А. В. Олифиров, К. А. Маковейчук // Безопасные информационные технологии : Сборник трудов Двенадцатой международной научно-технической конференции, Москва, 01–02 ноября 2023 года. – Москва: Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), 2023. – С. 124-129. – EDN DGWFIV.

Information Security System of the Digital Payments Ecosystem: Optimization of Protection Measures

Alexander V. Olifirov, Krystina A. Makoveichuk, and Nikita I. Potapovich

***Abstract* — The article proposes an incremental approach to the optimization of protection measures of digital payment ecosystems. It is established that the basis for the development of national economies are information and digital technologies, distributed ledger system and platform solutions, which form new technological ecosystems. It is shown that in modern conditions payment ecosystems are transformed to work with digital national currencies. It is noted that the main problem of realizing the concept of central bank digital currency is to ensure information security of its ecosystem. The target model of creation and use of the payment ecosystem of digital currency of the central bank is defined. The model of payment ecosystem based on payment transaction template is proposed. It is shown that as a result of decomposition based on the incremental approach, it is possible to identify threats and defense measures for each sub-template and each target class of the payment ecosystem of central bank digital currency, that is, it is possible to investigate how each element and service of the CBDC payment ecosystem can be attacked and how this attack can be deflected and weakened. An economic and mathematical model is constructed to optimize the resulting complete set of protection measures for the digital payment ecosystem.**

***Keywords* — Incremental analysis, information security, payment protection measures, central bank digital currency, digital payment ecosystem, digital technology, economic and mathematical model.**

REFERENCES

[1] Barabanov A.V., Dorofeev A.V., Markov A.S., Cirlov V.L. Sem` bezopasny`x informacionny`x texnologij / Pod. red. A.S.Markova. M.: DMK Press, 2017. 224 s. (In Russian)

[2] Miloslavskaya N.G., Tolstoj A.I. Upravlenie informacionnoj bezopasnost`yu. M.: NIYaU MIFI, 2020. – 536 s. (In Russian)

[3] Olifirov A., Makoveichuk K., Petrenko S. Cybersecurity measures of the digital payment ecosystem. In Selected Papers of 11th International Scientific and Technical Conference on Secure Information Technologies (BIT 2021). CEUR Workshop Proceedings, 2021, Vol-3035, pp. 133-142.

[4] Brantly, A. F. Risk and uncertainty can be analyzed in cyberspace, Journal of Cybersecurity, volume 7, issue 1, 2021, tyab001. DOI: 10.1093/cybsec/tyab001.

[5] Yu, H., Hsi, K., & Kuo, P. (2002). Electronic payment systems: an analysis and comparison of types. Technology in Society, 24, pp. 331-347. DOI: 10.1016/S0160-791X(02)00012-X.

[6] Raharja, S. U. J., Muhyi, H. A., Herawaty, T. Digital payment as an enabler for business opportunities: A go-pay case study. Review of Integrative Business and Economics Research, 9(1) (2020), pp. 319-329. URL: http://buscompress.com/uploads/3/4/9/8/34980536/riber_9-s1_25_b19-102_319-329.pdf.

[7] Staykova, Kalina & Damsgaard, Jan. (2016). Adoption of Mobile Payment Platforms: Managing Reach and Range. Journal of theoretical and applied electronic commerce research, 11(3), pp. 66-85. DOI: 10.4067/S0718-18762016000300006.

[8] E`kosistemy`: podxody` k regulirovaniyu. Doklad dlya obshhestvenny`x konsul`tacij, Moskva, 2021. https://www.cbr.ru/Content/Document/File/119960/Consultation_Paper_02042021.pdf. (In Russian)

[9] Khomenko E.G. Electronic payment systems in Russia and in foreign countries. Actual Problems of Russian Law, 2019, (8):159-164. https://doi.org/10.17803/1994-1471.2019.105.8.159-164. (In Russian)

[10] Lin, Wan R., Lin, C.-H., & Ding, Y.-H. (2020). Factors affecting the behavioral intention to adopt mobile payment: An empirical study in Taiwan. Mathematics, 8(10), 1851. https://doi.org/10.3390/math8101851

[11] "Koncepciya cifrovogo rublya" (podgotovlena Bankom Rossii). – URL: http://www.consultant.ru/document/cons_doc_LAW_381918/ (data obrashheniya: 01.09.2021).

[12] Maslennikov V.V., Larionov A.V. Digital Currencies: Conceptualization of Risks and Regulatory Opportunities. The world of new economy, 2021, 15(4):16-28. https://doi.org/10.26794/2220-6469-2021-15-4-16-28. (In Russian)

[13] Agur I., Lavayssière X., Bauer G. V., Deodoro J., Peria S. M., Sandri D., Tourpe H. Lessons from crypto assets for the design of energy efficient digital currencies. Ecological Economics, 2023, Vol-212. https://doi.org/10.1016/j.ecolecon.2023.107888.

[14] Gilbert S., Loi H. Digital Currency Risk. International Journal of Economics and Finance, 2018, Vol-10, No. 2. DOI: 10.5539/ijef.v10n2p108.

[15] Olifirov A.V., Makoveichuk K.A., Petrenko S.A. Integration of cyber security into the Smart Grid operational risk management system. In Selected Papers of the 4th All-Russian Scientific and Practical Conference with International Participation "Information Systems and Technologies in Modeling and Control" (ISTMC 2019). CEUR Workshop Proceedings, 2019, Vol-2522, pp. 132-144. URL: https://ceur-ws.org/Vol-2522/paper14.pdf.

[16] Petrenko, A. A., Petrenko, S. A., Makoveichuk, K. A., Olifirov, A. V. Methodological recommendations for the cyber risks management, CEUR Workshop Proceedings, 2021, Vol-2914, pp. 234-247. URL: http://ceur-ws.org/Vol-2914/paper20.pdf.

[17] Petrenko, S., Petrenko, A., Makoveichuk, K.A., Olifirov, A. (2021). Development of a Cyber-Resistant Platform for the Internet of Things Based on Dynamic Control Technology. In: Singh, P.K., Veselov, G., Vyatkin, V., Pljonkin, A., Dodero, J.M., Kumar, Y. (eds) Futuristic Trends in Network and Communication Technologies. FTNCT 2020. Communications in Computer and Information Science, vol 1395. Springer, Singapore. https://doi.org/10.1007/978-981-16-1480-4_13.

[18] Petrenko, S. A., Makoveichuk, K. A., Olifirov, A. V. Concept of cyber immunity of industry 4.0. CEUR Workshop Proceedings, 2019, Vol-2603, pp. 93-99. URL: http://ceur-ws.org/Vol2603/paper20.pdf.

[19] Petrenko, S., Makoveichuk, K., Olifirov, A. (2020). New Methods of the Cybersecurity Knowledge Management Analytics. In: Sukhomlin, V., Zubareva, E. (eds) Convergent Cognitive Information Technologies. Convergent 2018. Communications in Computer and Information Science, vol 1140. Springer, Cham. https://doi.org/10.1007/978-3-030-37436-5_27.

[20] Bank Rossii. Osnovny`e tipy` komp`yuterny`x atak v kreditno-finansovoj sfere v 2019–2020 godax. Moskva, 2021, URL: https://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf. (In Russian)

[21] Boholm, M. Twenty-five years of cyber threats in the news: a study of Swedish newspaper coverage (1995–2019), Journal of Cybersecurity, Volume 7, Issue 1, 2021, tyab016, https://doi.org/10.1093/cybsec/tyab016.

[22] Agrafiotis. I., Nurse, J. R. C., Goldsmith M., Creese, S., Upton, D, A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, Journal of Cybersecurity, Volume 4, Issue 1, 2018, tyy006, https://doi.org/10.1093/cybsec/tyy006.

[23] Yankovskij R. M. Kriptovalyuty` v rossijskom prave: surrogaty`, "inoe imushhestvo" i cifrovy`e den`gi // Pravo. Zhurnal Vy`sshej shkoly` e`konomiki. 2020. № 4. URL:

https://cyberleninka.ru/article/n/kriptovalyuty-v-rossiyskom-prave-surrogaty-inoe-imuschestvo-i-tsifrovye-dengi. (In Russian)

[24] Bauer V.P., Smirnov V.V. Institutional Features of the Development of Competitive Cryptocurrency. Finance: Theory and Practice. 2020;24(5):84-99. https://doi.org/10.26794/2587-5671-2020-24-5-84-99. (In Russian)

[25] Courtier, P., Thépaut, J.-N., Hollingsworth, A. A strategy for operational implementation of 4D-Var, using an incremental approach. Quarterly Journal of the Royal Meteorological Society, 1994, Vol-120, Issue 519, pp. 1367-1387. https://doi.org/10.1002/qj.49712051912.

[26] Sun, P., Li, X., & Ting, M. Y. Efficient incremental analysis of on-chip power grid via sparse approximation. In Proceedings - Design Automation Conference, 2011, pp. 676–681. https://doi.org/10.1145/2024724.2024878.

[27] Olifirov, A. V. Modeli upravleniya riskami e`konomicheskix informacionny`x sistem / A. V. Olifirov // Informacionny`e sistemy` i texnologii v modelirovanii i upravlenii : Materialy` vserossijskoj nauchno-prakticheskoj konferencii, Yalta, 05–07 iyulya 2017 goda / Otvetstvenny`x redaktor N.N. Olejnikov. – Yalta: Obshhestvo s ogranichennoj otvetstvennost`yu «Izdatel`stvo Tipografiya «Arial», 2017. – S. 465-470. – EDN YYVSVL. (In Russian)

[28] Olifirov, A. V. Organizacionno-texnicheskie mery` informacionnoj bezopasnosti cifrovoj valyuty` central`nogo banka / A. V. Olifirov, K. A. Makovejchuk // Bezopasny`e informacionny`e texnologii : Sbornik trudov Dvenadczatoj mezhdunarodnoj nauchno-texnicheskoj konferencii, Moskva, 01–02 noyabrya 2023 goda. – Moskva: Moskovskij gosudarstvenny`j texnicheskij universitet imeni N.E`. Baumana (nacional`ny`j issledovatel`skij universitet), 2023. – S. 124-129. – EDN DGWFIV. (In Russian)