Инженерный вестник Дона, №3 (2026)
ivdon.ru/ru/magazine/archive/n3y2026/10806

Моделирование архитектур обращения цифровых валют центральных банков и их информационная безопасность

И.А. Петров

Финансовый университет при Правительстве РФ

Аннотация: Цифровые валюты центральных банков являются третьей формой валюты, наряду с наличными и электронными деньгами. На момент 2026 года, в работу по исследованию введения в оборот собственных цифровых валют были вовлечены 86% из 65 ведущих центральных банков мира. Однако, центральные банки, при разработке цифровой валюты используют разные архитектуры обращения. В данной статье описаны эти архитектуры и проведено сравнение их информационной безопасности при помощи моделирования. Научная новизна заключается в создании математической модели платформы цифровых валют центральных банков с различными видами архитектур и сравнении их характеристик. Методами исследования в данной статье являются анализ, синтез данных с различных источников, индукция, моделирование. Результатом данной статьи является модель платформы цифровой валюты центральных банков и количественная оценка уровня информационной безопасности. Целью статьи является количественная оценка ключевых показателей безопасности гибридной архитектуры и полностью разрешённой архитектуры в условиях реальных профилей кибератак.
Ключевые слова: централизованная архитектура, центральные банки, информационная безопасность, моделирование, цифровой рубль, гибридная архитектура.

Введение

Цифровой рубль — это цифровая форма российской национальной валюты, которую Центральный Банк России (ЦБ) планирует выпускать в дополнение к существующим формам денег [1]. Цифровой рубль является третьей формой российской национальной валюты. Данная форма валюты представляет собой уникальный идентификационный номер (токен), который зарегистрирован на платформе ЦБ.

Согласно Федеральному конституционному закону от 23.07.2025 № 1-ФКЗ "О внесении изменений в статьи 31 и 32 Федерального конституционного закона "О судебной системе Российской Федерации" и статью 38 Федерального конституционного закона "О судах общей юрисдикции в Российской Федерации" поэтапное массовое внедрение цифрового рубля начнется с 1 сентября 2026 года. Однако, перспективы

внедрения **цифровых валют центральных банков** (ЦВЦБ) в разных странах неоднозначны, есть как очевидные достоинства, так и недостатки [2-3].

Основная часть

ЦБ РФ в качестве архитектуры обращения цифрового рубля выбрал гибридную архитектуру. Гибридная модель цифрового рубля представляет собой двухуровневую структуру, в которой участвуют центральный банк и финансовые организации. Рассмотрим реализацию этой модели на примере платформы цифрового рубля [4].

Эмитентом цифровой валюты выступает государство. Центральный банк открывает кошельки для финансовых организаций, которые, в свою очередь, открывают кошельки для своих клиентов на платформе цифровой валюты и осуществляют расчеты в цифровом рубле.

Финансовые организации занимаются привлечением клиентов и взаимодействием с ними.

Финансовые учреждения выполняют предусмотренные законодательством процедуры по борьбе с отмыванием доходов и финансированием терроризма.

Зачисление цифрового рубля происходит путем списания соответствующих безналичных средств в соотношении 1:1. Каждый клиент может открыть только один кошелек. Кошельки клиентов хранятся на платформе цифрового рубля и не отображаются на балансе финансовых организаций.

В таких государствах как Китай, Швеция, Ямайке и Нигерии уже существуют ЦВЦБ, и каждая отличается своей реализацией, как в экономическом отношении, так и в отношении информационной безопасности [5].

Целью моделирования следующая: Количественно оценить, как выбор между гибридной архитектурой и полностью разрешённой

(централизованной) архитектурой влияет на ключевые показатели безопасности в условиях реальных профилей кибератак.

В современной терминологии, особенно от ведущих вендоров (IBM, Oracle, Microsoft), разрешенная и гибридная архитектура центра обработки данных (ЦОД) — это стратегические подходы к организации хранения и обработки корпоративных данных. Давайте разберем по порядку.

1. Разрешенная архитектура

Суть: Это официально утвержденная IT-департаментом и архитекторами предприятия целевая архитектура для систем хранения данных. Она определяет "золотой стандарт" — как данные должны храниться, обрабатываться и управляться в идеальном состоянии компании.

Ключевые характеристики архитектуры:

Единый источник истины: В ее основе лежит централизованное хранилище данных, построенное по строгим правилам (схемы "звезда"/"снежинка", очищенные, интегрированные данные);

Контроль и управление: Жесткий контроль за качеством данных, безопасностью, доступом и процессами;

Предсказуемость: Обеспечивает стабильную, надежную основу для регламентированной отчетности (финансы, управленческая отчетность) и бизнес-аналитики;

"Официальная" аналитика: Это источник для всех официальных отчетов, которые требуют точности и согласованности;

Проблема, которую она решает: Хаос, вызванный множеством неконтролируемых, слабо связанных между собой источников данных и аналитических систем;

2. Гибридная архитектура

Суть: Это прагматичное признание реальности, что одной "разрешенной" архитектуры недостаточно. Она сочетает централизованный

контроль с гибкостью и скоростью, необходимыми для современных задач (анализ больших данных, эксперименты).

Гибридная архитектура явно включает в себя два "слоя" или "мира":

"Разрешенный" мир: Классический ЦОД для критически важных, структурированных данных и регламентной отчетности.

"Гибкий" мир**:** Среды для неструктурированных данных, быстрого прототипирования, исследований данных, работы с большими данными в форматах like Hadoop, data lakes (озера данных) на облачных платформах (Azure Data Lake Storage).

Этап 1: Подготовка и анализ входных данных из файла

Прежде чем строить модель, нужно понять, что у нас есть и как это использовать. Статистика показывает, что существенно увеличивается количество таргетированных кибератак на значимые объекты [6-7]. Поэтому мной была составлена база данных по операциям без согласия клиентов, основанная на данных, предоставленными ЦБ РФ за 2020 год [8] 2021 год [9], 2022 год [10], 2023 год [1] и 2024 год [12]. Также использовались данные, предоставленные компанией Positive Technologies [13]. Данные представляют собой временной ряд (2014-2024 гг.) по месяцам и кварталам. (рисунок 1)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Год	Месяц	Квартал	перераций,	ство инцид	инженер	фишинг	ВПО	DDoS	ные атак	отвращ	ерщенны	енных сре	от кибер	от кибер
2014	1	1	104554	10217	146	60	5	29	198	307	1094	18244	4695869	1486235
2014	2	1	104605	10654	138	59	7	30	177	321	1040	17005	4434226	1482682
2014	3	1	106041	11129	136	61	6	31	181	322	1066	16751	4869905	1592203
2014	4	2	99555	14075	100	40	16	20	78	216	1248	10984	4940580	3376703
2014	5	2	107532	13354	104	40	16	20	75	205	1426	10120	4700887	3445893
2014	6	2	110213	13571	106	40	15	20	76	199	1426	9896	4958533	3177404
2014	7	3	155541	20057	172	67	4	38	123	360	1017	27080	4749765	4643008
2014	8	3	157377	20628	180	70	4	37	122	381	962	25863	5145990	4869753
2014	9	3	146482	19193	178	73	3	35	129	359	1021	25057	5104245	4709459
2014	10	4	187881	23216	219	95	7	50	141	448	1762	32263	4917005	5093180
2014	11	4	173967	21471	226	98	7	45	146	418	1907	31606	5046905	5138188
2014	12	4	185652	21191	235	97	7	45	149	434	1972	31131	5236090	4768632
2015	1	1	104864	24992	164	81	47	61	42	807	1867	42177	5295018	4700579
2015	2	1	105555	23248	169	89	49	62	41	778	1832	40039	4944611	5045023
2015	3	1	104981	23971	156	84	51	62	41	760	1765	42442	5060371	4954398
2015	4	2	93430	21489	197	67	29	20	104	638	2330	44216	4993649	5038155
2015	5	2	88426	19862	185	61	30	19	110	690	2311	40363	5222571	5356178
2015	6	2	89644	20305	185	61	30	19	111	659	2346	40299	5183780	5205667
2015	7	3	94936	22265	259	98	30	25	33	1221	3265	41084	4970105	5070563
2015	8	3	103325	23909	270	90	29	25	33	1063	2865	47353	5199691	5487202
2015	9	3	101439	22952	260	90	28	24	32	1065	2857	47537	5430204	5142235
2015	10	4	86002	19628	377	96	4	45	32	1624	1262	49361	4960901	5922335
2015	11	4	85974	19639	379	104	4	41	32	1627	1197	47786	5479250	5504220
2015	12	4	88424	18662	367	99	3	41	32	1625	1239	51827	5259849	5473445
2016	1	1	83778	21914	769	104	8	125	39	1815	3414	52223	5058568	5790890
2016	2	1	83053	20699	810	110	8	121	42	1920	3225	52030	5262205	5742512
2016	3	1	86269	20501	775	106	8	123	42	1952	3306	52736	5479227	5866598
2016	4	2	83252	21935	655	120	25	32	14	365	4272	51847	5352003	6220593
2016	5	2	82421	21275	615	110	26	33	14	380	4188	58723	5108581	5783615
2016	6	2	78327	22639	672	112	27	34	13	370	3994	59228	5539416	6065792
2016	7	3	94961	25314	406	123	18	119	64	2490	21181	50144	5445581	6525270
2016	8	3	99967	26831	414	119	18	114	64	2251	19023	49828	5312187	6151507
2016	9	3	98972	25319	434	121	18	111	61	2246	18770	47028	5742232	6063223
2016	10	4	90682	31472	815	129	52	50	115	2560	23465	53429	5482597	6495714
2016	11	4	94841	29422	778	128	52	46	103	2639	24171	50491	5771228	6469869
2016	12	4	98477	29383	751	127	52	49	103	2697	22184	52080	5646175	6444417
2017	1	1	78796	29480	1229	138	10	62	82	3008	26467	59176	5445318	6669299

Рис. 1. – База данных по операциям без согласия клиентов

Определим, что необходимо для создания модели архитектур ЦВЦБ.

Метрики угроз**:** Количество и тип инцидентов (социальная инженерия, фишинг, вредоносное программное обеспечение (ВПО), DDoS (Distributed Denial of Service – атака отказа в обслуживании), иные).

Метрики защищённости: Количество и объем предотвращенных атак.

Экономические метрики: Объем операций, ущерб, затраты на защиту, объем возмещенных средств.

Калибровка частоты и типа атак: Рассчитаем среднемесячную/квартальную вероятность возникновения атаки определенного типа на одну транзакцию или на условную "единицу инфраструктуры". Это станет входным распределением для генератора угроз в модели.

Определение эффективности защиты: Отношение Количество предотвращенных атак / Количество инцидентов даст нам базовую эффективность современных (традиционных) систем защиты. Это точка отсчета для наших архитектурных сценариев.

Оценка последствий: Финасовый ущерб / Объем операций или Ущерб / Инцидент — даст нам коэффициент ущерба, который мы будем модифицировать в зависимости от устойчивости архитектуры ЦВЦБ.

Тренды и сезонность: Выявим, есть ли рост сложности атак (например, смещение от DDoS к социальной инженерии). Это поможет задать сценарии развития угроз в будущем для прогнозного моделирования.

Этап 2: Архитектура агентной модели

Модель будет состоять из следующих агентов и модулей:

1. Агенты:

- Узлы (Валидаторы): Имеют тип: Центробанк, Уполномоченный банк (отобранный), Коммерческий банк (разрешённый). Параметры: вычислительная мощность, надёжность, степень доверия, доля в консенсусе;

•Пользователи: Генерируют транзакции. Могут быть скомпрометированы (агент "Злоумышленник");

•Злоумышленник: Не отдельный агент, а роль. Может контролировать группу скомпрометированных узлов или пользователей. Цель: сорвать консенсус или провести мошенническую транзакцию.

2. Модули:

•Генератор транзакций: Создает поток транзакций на основе трендов из данных (рост объема операций с 2014 по 2024);

•Генератор угроз: На основе статистики из файла генерирует события атак;

•DDoS: Случайный выбор узла-цели, снижение его доступности на время;

•ВПО/Социальная инженерия*:* Компрометация узла или пользователя. Узел начинает действовать злонамеренно (например, отправлять противоречивые голоса);

•"Иные атаки"*:* Моделирование сложных атак (например, на смарт-контракты протокола).

Модуль консенсуса: Реализует логику гибридного алгоритма консенсуса BFT (Byzantine Fault Tolerance, BFT) и, для сравнения, разрешённого алгоритма консенсуса PoA (Proof of Authority, PoA). Именно здесь проверяется гипотеза.

Гибридная архитектура: Небольшой набор отобранных валидаторов (ЦБ + крупные банки). Высокий порог для атаки (>2/3), но теоретически большая поверхность атаки на каждый узел.

Полностью разрешённая архитектура: Большое количество валидаторов (все банки). Порог атаки тот же, но злоумышленнику нужно скомпрометировать больше узлов, каждый из которых, возможно, защищен слабее.

Модуль безопасности: Применяет "защитные механизмы", характерные для архитектуры: быстрая смена ключей для гибридной, изоляция для разрешённой. Его эффективность — параметр, который мы будем варьировать.

Счётчик метрик: Собирает данные в ходе симуляции.

Этап 3: Ключевые параметры и сценарии моделирования

Настраиваемые параметры (исследуемые независимые переменные):

- Архитектура: Гибридная / Разрешённая;
- Количество валидаторов;
- Распределение долей/стейка: Централизованное (ЦБ 50%) или распределённое;
- Интенсивность атак: Берем из данных 2023-2024 гг. как базовый уровень;
- Тип преобладающей атаки: Изменяем пропорции в сторону целевых (ВПО) или массовых DDoS-атак;

Выходные метрики (зависимые переменные для оценки гипотезы):

- Время до сбоя консенсуса (среднее, наихудший случай).
- Вероятность успешной double-spend атаки.
- Доля скомпрометированных валидаторов до нарушения работы.

Этап 4: Процесс моделирования и валидации

Базовый прогон (Валидация модели):

Настраиваем модель так, чтобы она имитировала традиционную систему (клиент-банк). Задаём параметры атак и эффективности защиты на уровне, рассчитанном из данных за 2023-2024 гг. Запускаем симуляцию на условные 12 месяцев (144 такта).

Сравниваем полученные смоделированные значения количества инцидентов, ущерба и эффективности защиты с реальными данными из файла.

Основные прогоны (Проверка гипотезы):

Сценарий А: Запускаем модель с параметрами гибридной архитектуры цифрового рубля. Ниже, на рисунке 2, показана часть кода с описанием гибридной архитектуры.

```
if self.architecture == "hybrid":
    # Гибридная: 20% центральные, 30% уполномоченные, 50% коммерческие
    n_central = max(2, int(self.n_validators * 0.2))
    n_authorized = max(3, int(self.n_validators * 0.3))
    n_commercial = self.n_validators - n_central - n_authorized

    for i in range(n_central):
        security = random.uniform(0.85, 0.95)
        validators.append(BalancedValidator(i, "central", security))

    for i in range(n_authorized):
        security = random.uniform(0.75, 0.85)
        validators.append(BalancedValidator(n_central + i, "authorized", security))

    for i in range(n_commercial):
        security = random.uniform(0.65, 0.75)
        validators.append(BalancedValidator(n_central + n_authorized + i, "commercial", security))
```

Рис. 2. – Код модели гибридной архитектуры

Сценарий Б: Запускаем модель с параметрами полностью разрешённой архитектуры**.** Ниже, на рисунке 3, показана часть кода с описанием гибридной архитектуры.

```
else:  # permissioned
    # Разрешенная: более равномерное распределение
    for i in range(self.n_validators):
        if i < self.n_validators * 0.15:  # 15% высокозащищенные
            security = random.uniform(0.80, 0.90)
            vtype = "central"
        elif i < self.n_validators * 0.45:  # 30% средние
            security = random.uniform(0.70, 0.80)
            vtype = "authorized"
        else:  # 55% обычные
            security = random.uniform(0.60, 0.70)
            vtype = "commercial"

        validators.append(BalancedValidator(i, vtype, security))

return validators
```

Рис. 3. – Код модели разрешенной архитектуры

Для каждого сценария проводим N прогонов (например, 1000) с разными случайными семенами для статистической значимости. Далее фиксируем все выходные метрики.

Необходимо также провести стресс-тесты. Для этого увеличиваем интенсивность атак в 2, 5, 10 раз, а также меняем профиль угроз в сторону целевых атак на валидаторов. Смотрим, при каком уровне давления одна архитектура становится менее устойчивой, чем другая.

Этап 5: Анализ результатов и формулирование рекомендаций

На выходе мы получим для каждой архитектуры распределения ключевых метрик.

Гипотеза подтвердится, если для гибридной архитектуры вероятность успешной атаки будет статистически значимо ниже при том же или сопоставимом уровне атак.

При этом Индекс децентрализации будет выше некоторого приемлемого порога (например, что ни один участник не контролирует >33%).

В стресс-тестах гибридная архитектура будет "ломаться" позже или при более высоком пороговом значении атак.

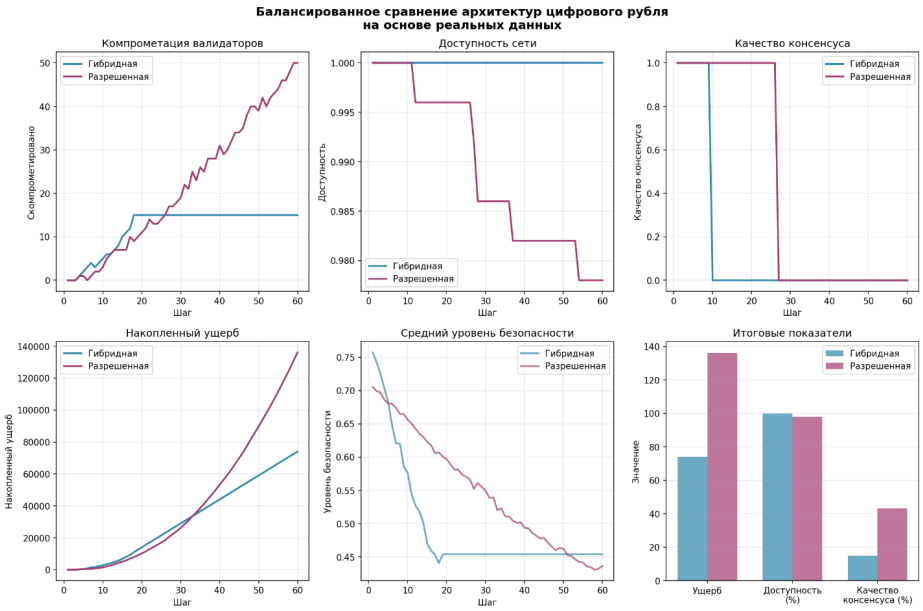

Рис. 4. – Балансированное сравнение архитектур цифрового рубля на основе реальных данных

```
================================================================================
АНАЛИЗ РЕЗУЛЬТАТОВ
================================================================================

ГИБРИДНАЯ:
  • Итоговый ущерб: 76,053
  • Скомпрометировано: 15/15
  • Доступность: 97.3%
  • Качество консенсуса: 11.7%

РАЗРЕШЕННАЯ:
  • Итоговый ущерб: 167,831
  • Скомпрометировано: 50/50
  • Доступность: 98.9%
  • Качество консенсуса: 33.3%

================================================================================
СРАВНИТЕЛЬНЫЙ АНАЛИЗ
================================================================================

✓ ГИБРИДНАЯ АРХИТЕКТУРА ЭФФЕКТИВНЕЕ:
  • Снижение ущерба: 54.7% (91,777)

✓ ГИПОТЕЗА ПОДТВЕРЖДЕНА:
  Гибридная архитектура обеспечивает более высокий уровень
  безопасности при сохранении децентрализации

================================================================================
РЕКОМЕНДАЦИИ ДЛЯ ЦИФРОВОГО РУБЛЯ
================================================================================
1. Оптимальная архитектура: ГИБРИДНАЯ
2. Рекомендуемое количество валидаторов: 15
3. Критические меры безопасности:
   • Многофакторная аутентификация
   • Регулярное обновление систем защиты
   • Мониторинг в реальном времени
   • Резервные механизмы консенсуса
4. Рекомендуемый порог консенсуса: 2/3 голосов
✓ Данные Гибридная сохранены в balanced_Гибридная_20260105_113804.csv
✓ Данные Разрешенная сохранены в balanced_Разрешенная_20260105_113804.csv

================================================================================
АНАЛИЗ ЗАВЕРШЕН
================================================================================
```

Рис. 5. – Анализ результатов модели

На основе рисунков 4 и 5 можно сделать следующие выводы:

Гибридная архитектура оказалась безопаснее и эффективнее. Количество компрометаций после 30 шага сильно снижается в сравнении с разрешенной архитектурой. Ущерб также ниже у гибридной архитектуры.

Доступность почти одинаковая, но у гибридной архитектуры она чуть выше;

Качество консенсуса ниже у гибридной архитектуры, что вполне объяснимо составом участников архитектуры.

Представленная модель имеет свои ограничения:

Упрощенная модель сети - не учитывает сетевые задержки и географическое распределение;

Детерминированные параметры - случайность ограничена случайными числами;

Линейная зависимость ущерба - в реальности может быть нелинейной;

Статическое распределение валидаторов - не адаптируется в ходе симуляции.

Как было указано в источнике [14], ЦБ РФ, в качестве архитектуры платформы цифрового рубля, выбрал гибридную архитектуру. Это решение является верным, что подтверждает построенная модель.

Заключение

Была составлена модель двух архитектур обращения ЦВЦБ, разрешенной и гибридной. Также была составлена база данных по операциям без согласия клиентов с 2014 по 2024 гг. Сравнительный анализ показал то, что гибридная архитектура обладает лучшей информационной безопасностью по сравнению с разрешенной. Гибридная архитектура обладает меньшим количеством компрометаций валидаторов, большей доступностью сети. Поэтому выбор в качестве гибридной архитектуры для цифрового рубля оказался верным.

Литература

1. George Pantelopoulos. Central Bank Digital Currencies (CBDC) / Between Payments and Credit. – 2025. – pp. 201-251. // URL: researchgate.net/publication/392916188_Central_Bank_Digital_Currencies_CBDC
2. Bhatia, N. (2021) Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies, 180 p.
3. Цифровой рубль. URL: cbr.ru/fintech/dr/ (дата обращения 10.01.2026 г.)
4. Цифровой рубль. Доклад для общественных дискуссий // URL: cbr.ru/StaticHtml/File/112957/Consultation_Paper_201013.pdf
5. Петров, И. А. Сравнение информационной безопасности цифровых валют центральных банков различных государств // Информатизация и

связь. – 2025. – № 4. – С. 136-143. – DOI 10.34219/2078-8320-2025-16-4-136-143. – EDN UYISKU

6. Чибинев Н.Н., Ляшенко Н.В. Кибератака как новый вид чрезвычайных ситуаций // Инженерный вестник Дона, 2024, №7. URL: ivdon.ru/ru/magazine/archive/n7y2024/9323.
7. Курейчик В.М., Сахарова О.Н., Пирожков С.С. Угрозы в области хранения данных // Инженерный вестник Дона, 2021, №7. URL: ivdon.ru/ru/magazine/archive/n7y2021/7111
8. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств // URL: cbr.ru/statistics/ib/review_1q_2q_2020
9. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств // URL: cbr.ru/statistics/ib/review_3q_2021
10. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств // URL: cbr.ru/statistics/ib/review_3q_2022
11. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств // URL: cbr.ru/statistics/ib/review_3q_2023/
12. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств // URL: cbr.ru/statistics/ib/review_3q_2024
13. Актуальные киберугрозы: III квартал 2024 года // URL: ptsecurity.com/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda
14. Концепция цифрового рубля // URL: cbr.ru/content/document/file/120075/concept_08042021.pdf

References

1. George Pantelopoulos. Central Bank Digital Currencies (CBDC). Between Payments and Credit. – 2025. – pp. 201-251. URL: researchgate.net/publication/392916188_Central_Bank_Digital_Currencies_CBDC

2. Bhatia, N. (2021). Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies, 180 p.

3. Cifrovoj rubl' [Digital Ruble]. URL: cbr.ru/fintech/dr/

4. Cifrovoj rubl'. Doklad dlya obshchestvennyh diskussij [Digital Ruble. Report for public discussion]. URL: cbr.ru/StaticHtml/File/112957/Consultation_Paper_201013.pdf

5. Petrov, I. A. Informatizaciya i svyaz'. 2025, № 4. pp. 136-143. DOI 10.34219/2078-8320-2025-16-4-136-143.

6. Chibinev N.N., Lyashenko N.V. Inzhenernyj vestnik Dona, 2024, №7. URL: ivdon.ru/ru/magazine/archive/n7y2024/9323

7. Kurejchik V.M., Saharova O.N., Pirozhkov S.S. Inzhenernyj vestnik Dona, 2021, №7. URL: ivdon.ru/ru/magazine/archive/n7y2021/7111

8. Obzor otchetnosti ob incidentah informacionnoj bezopasnosti pri perevode denezhnyh sredstv [Review of information security incidents related to money transfers]. URL: cbr.ru/statistics/ib/review_1q_2q_2020

9. Obzor otchetnosti ob incidentah informacionnoj bezopasnosti pri perevode denezhnyh sredstv [Review of information security incidents related to money transfers]. URL: cbr.ru/statistics/ib/review_3q_2021

10. Obzor otchetnosti ob incidentah informacionnoj bezopasnosti pri perevode denezhnyh sredstv [Review of information security incidents related to money transfers]. URL: cbr.ru/statistics/ib/review_3q_2022

11. Obzor otchetnosti ob incidentah informacionnoj bezopasnosti pri perevode denezhnyh sredstv [Review of information security incidents related to money transfers].URL: cbr.ru/statistics/ib/review_3q_2023

12. Obzor otchetnosti ob incidentah informacionnoj bezopasnosti pri perevode denezhnyh sredstv [Review of information security incidents related to money transfers]. URL: cbr.ru/statistics/ib/review_3q_2024

13. Aktual'nye kiberugrozy: III kvartal 2024 goda [Current Cyber Threats: Q3 2024]. URL: ptsecurity.com/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/

14. Koncepciya cifrovogo rublya [The concept of the digital ruble]. URL: cbr.ru/content/document/file/120075/concept_08042021.pdf

Авторы согласны на обработку и хранение персональных данных.

Дата поступления: 19.01.2026

Дата публикации: 25.02.2026