АРБ Ассоциация Российских Банков

ЦИБИТ

Киберкомплаенс для цифрового рубля: как выполнить перекрёстные требования Банка России, ФСТЭК России и ФСБ России

Открытый вебинар

Ассоциация Российских Банков

ЦИБИТ

01 **Синергия требований**

Как интегрировать стандарты ЦБ РФ, ФСТЭК России и ФСБ России в единую систему управления рисками для проектов с цифровым рублём

02 **ГОСТ 57580 на практике**

Как новые стандарты помогают унифицировать подходы к информационной безопасности и обеспечить непрерывность бизнес-процессов

03 **Операционная надёжность**

Фокус на оценке рисков и построении отказоустойчивых процессов, критичных для платформы цифрового рубля

04 **Ответ на вызовы**

Как обеспечить постоянное соответствие требованиям в условиях регулярных обновлений нормативной базы

Ассоциация Российских Банков

ЦИБИТ

Цифровой рубль: комплексный вызов для информационной безопасности

Велякин Алексей Владимирович

Руководитель Дирекции проектов ЦИБИТ

Цифровой рубль — вызов для информационной безопасности

- Технологический и финансовый прорыв;
- Платформа ЦБ станет объектом **критической инфраструктуры (КИИ);**
- Пристальное внимание и строгие требования ключевых регуляторов: ФСТЭК России и ФСБ России.

Ландшафт регулирования

ФСТЭК России	ФСБ России
Сфера: техническая защита информации (некриптографическая).	**Сфера**: криптографическая защита информации (СКЗИ).
Ключевой документ: новый приказ № 117 (с 01.03.2026) для ГИС.	**Вектор**: усиление контроля за цифровыми коммуникациями (пример — СОРМ для чатов).
Фокус: защита ИТ-инфраструктуры, контроль доступа, обнаружение вторжений, безопасность виртуальных сред.	**Для цифрового рубля**: использование только сертифицированных СКЗИ, обеспечение доступа уполномоченных органов.

Требования ФСТЭК России

- **Классификация:** Объект КИИ **1-го уровня значимости**;
- **Защита от НСД:** Многоуровневая модель (сетевой, транспортный, прикладной уровень);
- **Аттестация:** с обязательным **моделированием угроз** (DDoS, MITM-атаки);
- **Специфика для платформы Цифрового рубля:**
  - Изоляция нод распределённого реестра;
  - Контроль целостности смарт-контрактов.

Требования ФСБ России

- **Криптографическая защита:**
  - Обязательное использование сертифицированных СКЗИ;
  - Защита ключей электронной подписи;
  - Аудит всех криптоопераций.
- **Контрразведывательные меры:**
  - Специальные допуски для персонала;
  - Шифрование каналов передачи транзакций цифрового рубля.

АРБ Ассоциация Российских Банков

ЦИБИТ

От точечного комплаенса к единой системе

Операционная эффективность

Унификация процессов снижает нагрузку на персонал

Повышение управляемости

Централизованная система, готовая к проверкам любого регулятора

Снижение затрат

Исключение дублирования мер и функций

Выявление пересекающихся требований регуляторов

Требование	ФСТЭК России	ФСБ России	Банк России
Идентификация и аутентификация	Для всех участников платформы		
Контроль целостности	Защита КИИ		Неизменность транзакций
Регистрация событий	Мониторинг и аудит	Аудит-трейл для запросов	
Защита каналов		Криптография	Технические требования

Компонент	Назначение и связь с требованиями
1. Межсетевые экраны уровня гипервизора (NGFW)	Создание контура безопасности. Закрывает: требования ФСТЭК к защите виртуализации, изоляцию компонентов платформы.
2. Сертифицированные СКЗИ	Шифрование данных и каналов, ЭП. Жёсткое требование ФСБ. Применение как на периметре, так и внутри платформы.
3. Отечественная SIEM-система	Централизованный сбор и анализ событий безопасности. Ключ для обоих регуляторов: мониторинг (ФСТЭК) + аудит-трейл (ФСБ). Автоматизация отчётности.

Ключевые технологические компоненты интегрированной системы

АРБ Ассоциация Российских Банков

ЦИБИТ

Практические шаги

1. Совместный анализ требований;
2. Архитектурный подход «безопасность по дизайну»;
3. Выбор сертифицированной экосистемы;
4. Автоматизация комплаенса.

Заключение

- Цифровой рубль работает в уникально жёстком регуляторном поле.
- Успех зависит от целостной системы, а не точечных мер.
- Технологии (NGFW, СКЗИ, SIEM) должны быть глубоко интегрированы друг с другом и в технологические процессы.

Результат: не только успешное прохождение проверок, но и создание устойчивой платформы для новой формы национальной валюты.

Ассоциация Российских Банков

ЦИБИТ

ГОСТ 57580 и автоматизированный аудит: Единая система безопасности для цифрового рубля

Калугина Александра Владимировна

Эксперт Департамента финансового комплаенса ЦИБИТ

ГОСТ Р 57580 – недостающее звено для систематизации

Решает главную задачу:

объединяет разрозненные требования в единый каркас.

Метод:

риск-ориентированный процесс, встроенный в цикл PDCA (Plan-Do-Check-Act).

Результат:

превращает комплаенс в цикличный процесс управления.

Как это работает для цифрового рубля?

- **PDCA как единый ритм работы:**
  Планирование → Внедрение → Контроль → Коррекция.
- **Фокус на бизнес-процессы:**
  Защищаем не «железо», а непрерывность эмиссии, перевода, обмена.
  Выстраиваем универсальные сценарии восстановления.
- **Единые правила и метрики:**
  Один набор политик информационной безопасности и отчетности для всех регуляторов.

Автоматизированная платформа оценки соответствия

1. **Цель**

Превратить эпизодический аудит в непрерывный процесс управления.

2. **Суть**

Создание единой цифровой модели соответствия организации.

АРБ Ассоциация Российских Банков

ЦИБИТ

Этапы работы платформы

Единая форма аудита

Интеграция ключевых положений Банка России в одну модель

Комплексная оценка контура

Сквозная оценка всего контура безопасности

Автоматизация сбора информации

Объективные данные без человеческого фактора

Автоформирование отчётности

Автоматическое заполнение Формы 071 ЦБ РФ

Расчёт уровня защищенности

Расчёт показателя соответствия

Код	Оценка
1	2
ЕПОП- 683	н/о
ЕПОР- 683	н/о
ЕПОК- 683	н/о
ЕПОС- 683	н/о
ЕПО- 683	н/о
ПО ОС Признак, характеризующий использование прикладного программного обеспечения автоматизированных систем и приложений, которые сертифицированы в системе сертификации ФСТЭК России или в отношении которых проведена оценка соответствия требованиям к оценочному уровню доверия (далее - ОУД)	н/о

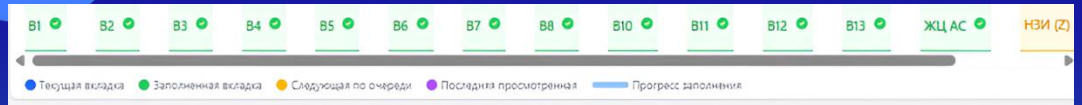
Оценки соответствия по направлению "Безопасность программного обеспечения" - 683

Код	Оценка
1	2
ЕПОП- 719	н/о
ЕПОР- 719	н/о
ЕПОК- 719	н/о
ЕПОС- 719	н/о
ЕПО- 719	н/о
ПО ОС Признак, характеризующий использование прикладного программного обеспечения автоматизированных систем и приложений, которые сертифицированы в системе сертификации ФСТЭК России или в отношении которых проведена оценка соответствия требованиям к оценочному уровню доверия (далее - ОУД)	н/о

Оценки соответствия по направлению "Безопасность программного обеспечения" - 719

Код	Оценка
1	2
ЕПОП- all	н/о
ЕПОР- all	н/о
ЕПОК- all	н/о
ЕПОС- all	н/о
ЕПО- all	н/о
ПО ОС Признак, характеризующий использование прикладного программного обеспечения автоматизированных систем и приложений, которые сертифицированы в системе сертификации ФСТЭК России или в отношении которых проведена оценка соответствия требованиям к оценочному уровню доверия (далее - ОУД)	н/о

Оценки соответствия по направлению "Безопасность программного обеспечения" - all



НАИМЕНОВАНИЕ ПРОЦЕССА СИСТЕМЫ	ОЦЕНКА, ХАРАКТЕРИЗУЮЩАЯ ВЫБОР ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР СИСТЕМЫ ЗИ	ОЦЕНКА ПО НАПРАВЛЕНИЯМ ЗИ СИСТЕМЫ ОРГАНИЗАЦИИ И УПРАВЛЕНИЯ ЗИ				КАЧЕСТВЕННАЯ ОЦЕНКА УРОВНЯ СООТВЕТСТВИЯ	ЧИСЛОВОЕ ЗНАЧЕНИЕ ОЦЕНКИ
		ПЛАНИРОВАНИЕ	РЕАЛИЗАЦИЯ	КОНТРОЛЬ	СОВЕРШЕНСТВОВАНИЕ		
Процесс 1 "Обеспечение защиты информации при управлении доступом"	0.88	1	0.8	0.91	1	четвёртый	0.89
Процесс 2 "Обеспечение защиты вычислительных сетей"	1.00	1	0.9	0.88	1	пятый	0.97
Процесс 3 "Контроль целостности и защищенности информационной инфраструктуры"	0.79	1	0.9	1	1	четвёртый	0.88
Процесс 4 "Защита от вредоносного кода"	1.00	1	0.9	0.96	1	пятый	0.98
Процесс 5 "Предотвращение утечек информации"	1.00	0.9	0.82	0.91	1	пятый	0.94
Процесс 6 "Управление инцидентами защиты информации"	0.82	1	0.9	1	1	четвёртый	0.89
Процесс 7 "Защита среды виртуализации"	0.92	0.9	0.85	0.86	1	четвёртый	0.9
Процесс 8 "Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств"	0.91	0.9	0.65	0.95	1	четвёртый	0.87
					Применение организационных и технических мер ЗИ на этапах жизненного цикла АС		0.78
					Количество нарушений ЗИ		н/о
					Итоговая оценка соответствия ЗИ		0.9

Заключение

- Принцип: «Соответствие по умолчанию».
- Трансформация: от формального и стрессового события — к постоянному и прозрачному процессу.

Результат: автоматизированный, системный и непрерывный подход — основа безопасности национальной цифровой валюты.

Ассоциация Российских Банков

ЦИБИТ

Комплаенс для цифрового рубля: от статьи расходов к драйверу роста

Колодина Евгения Викторовна

Первый заместитель Генерального директора ЦИБИТ

Эффективность как результат

Проблема: «ручной» аудит в проекте цифрового рубля — это якорь.

Решение:

платформа оценки ЦИБИТ — преимущества, измеряемые в деньгах.

АРБ Ассоциация Российских Банков

ЦИБИТ

Высокая эффективность и скорость

Автоматизация до **80%** рутинной работы

Сокращение цикла оценки

Экономия сотен человеко-часов

Высвобождение ресурсов

Полная прозрачность и объективность

- Исключён человеческий фактор;
- Проактивная защита: вы видите уязвимость до инцидента;
- Проверки по единым, встроенным методикам;
- Спасённые миллионы на ликвидацию ущерба и защиту репутации

Ассоциация Российских Банков

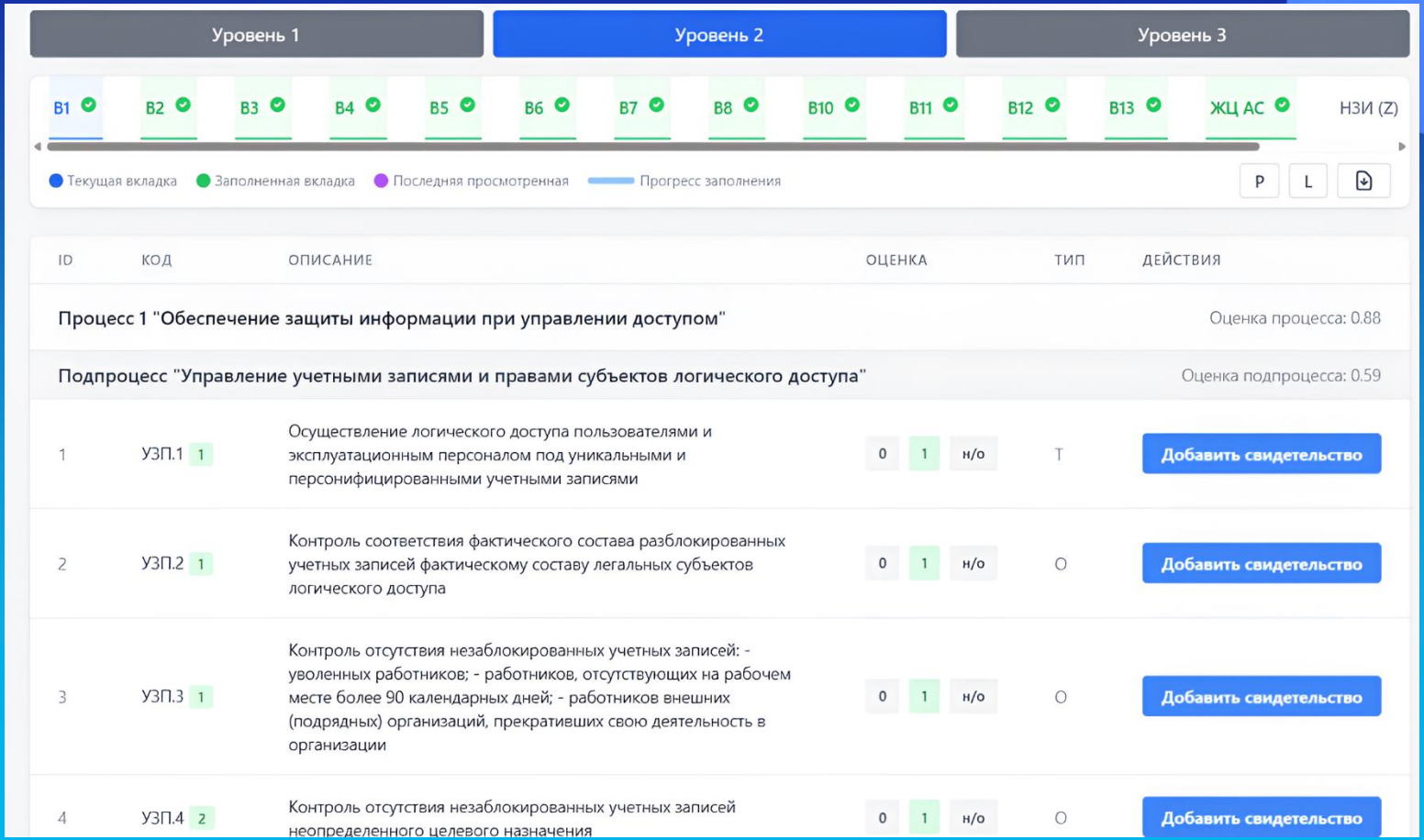
ЦИБИТ

Гибкая архитектура

Управление рисками в реальном времени

Цикличный процесс постоянного контроля

Сохранение истории и доказательств

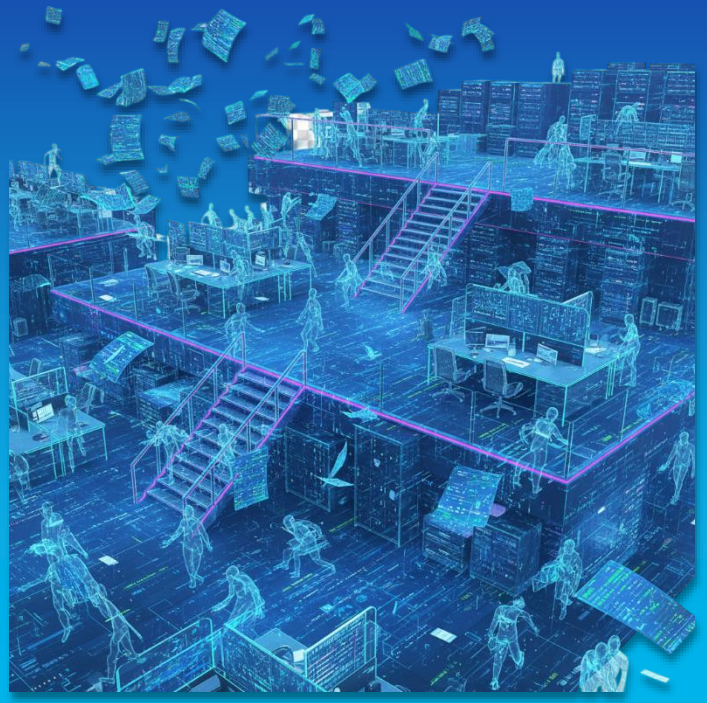


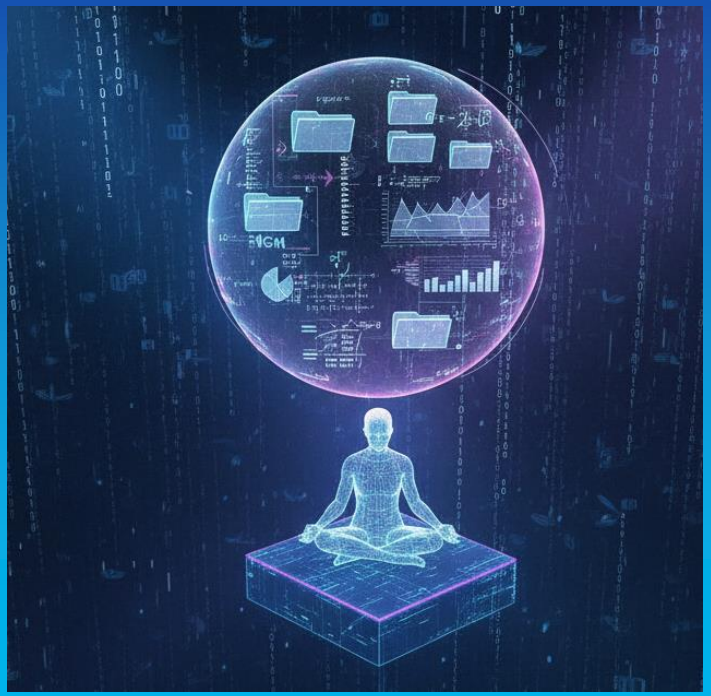
ID	КОД	ОПИСАНИЕ	ОЦЕНКА	ТИП	ДЕЙСТВИЯ
Процесс 1 "Обеспечение защиты информации при управлении доступом"					Оценка процесса: 0.88
Подпроцесс "Управление учетными записями и правами субъектов логического доступа"					Оценка подпроцесса: 0.59
1	УЗП.1 1	Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями	0 1 н/о	Т	Добавить свидетельство
2	УЗП.2 1	Контроль соответствия фактического состава разблокированных учетных записей фактическому составу легальных субъектов логического доступа	0 1 н/о	О	Добавить свидетельство
3	УЗП.3 1	Контроль отсутствия незаблокированных учетных записей: - уволенных работников; - работников, отсутствующих на рабочем месте более 90 календарных дней; - работников внешних (подрядных) организаций, прекративших свою деятельность в организации	0 1 н/о	О	Добавить свидетельство
4	УЗП.4 2	Контроль отсутствия незаблокированных учетных записей неопределенного целевого назначения	0 1 н/о	О	Добавить свидетельство

АРБ Ассоциация Российских Банков

ЦИБИТ

Бессистемный хаос VS Аккуратная система





Удобство:

- Вся информация — в едином структурированном пространстве;
- Каждое доказательство привязано к пункту стандарта;
- Поиск: не дни и часы, а секунды!

Итоговый результат:

«Догоняющий», который тратит ресурсы на отчётность

Проактивный лидер

АРБ Ассоциация Российских Банков

ЦИБИТ

Ключевое звено в цепи безопасности — ЧЕЛОВЕК

80% инцидентов из-за человеческого фактора

Цифровой рубль: цена ошибки возрастает в разы

Регуляторы ставят кадры и обучение во главу угла.

ФСТЭК России	Банк России	ФСБ России
Приказ №117 (с 01.03.2026): 30% специалистов ИБ обязаны иметь официальный диплом.	Требует экспертизы по криптографии и архитектуре цифрового рубля.	Лицензирует работу с шифрованием.

АРБ Ассоциация Российских Банков

ЦИБИТ

Указ Президента № 250

ужесточает персональную ответственность за информационную безопасность, требуя, чтобы этим занимался высокопоставленный руководитель с подтверждённой квалификацией, а в организации существовало профильное подразделение, ориентированное на практическую защиту

Последствия невыполнения: миллионные штрафы и риск остановки операций с цифровым рублем

АРБ Ассоциация Российских Банков

ЦИБИТ

Три ключевых вызова:

- Кадровый голод. Дефицит архитекторов, инженеров, экспертов по российскому стеку.
- Новая культура безопасности. Требуется на всех уровнях: от операциониста до топ-менеджера.
- Жёсткие сроки. Подключение с сентября 2026, полное внедрение цифрового рубля к 2028. На обучение — месяцы.

АРБ Ассоциация Российских Банков

ЦИБИТ

Что делать?

АРБ Ассоциация Российских Банков

ЦИБИТ

Системный подход:

- ✓ Проверка соответствия;
- ✓ Матрица компетенций;
- ✓ Регулярные тренировки.

Что делать дальше? Решение ЦИБИТ

1. Обучение (привести в соответствие):

- Программы для 30% специалистов (по ФСТЭК №117).

АРБ Ассоциация Российских Банков ЦИБИТ

Программа профессиональной переподготовки «Информационная безопасность. Управление жизненным циклом шифровальных (криптографических) средств»

- ✓ Согласована с ФСБ России;
- ✓ Объём программы составляет 1260 академических часов;
- ✓ В учебный план входят как правовые аспекты ИБ и основы криптографии, так и специализированные модули по порядку разработки, производства, распространения и эксплуатации шифровальных средств (СКЗИ)

Кадровое агентство

- Партнёр по комплаенсу, готовый закрыть ваши кадровые риски.
- Поиск специалистов «под ключ» с учётом требований регуляторов и возможностью оперативно закрыть пробел в навыках кандидата.

Культура безопасности (для всех)

Обучение и повышение осведомленности в области информационной безопасности для всех сотрудников

Ваш путь к лидерству:

Платформа оценки ЦИБИТ

Технологическое ядро

Инвестиции в кадры

Стратегическое вложение

АРБ Ассоциация Российских Банков

ЦИБИТ

Мы помогаем соответствовать требованиям!

www.cibit.ru
info@cibit.ru
+7 (495) 792-80-80
г. Москва, ул. Тушинская, д. 8