#PAYMENTSECURITY

Безопасные облачные решения для финтеха

От требований регулятора до реальной архитектуры

Александр Мизерин
Эксперт по информационной безопасности, Yandex Cloud

Василий Пургин
Архитектор решений, Affirmative Systems

5–6 августа 2026

План доклада

01 Зачем финтеху облако

02 Что мешает заехать

03 Что нужно сделать банку

04 Как устроена архитектура и безопасность

05 Практика и результат

ИНФОРМАЦИЯ

Почему я об этом рассказываю

9 лет

В банковском ИБ: несколько банков, комплаенс, техническая защита, криптография.

Я был по ту сторону — тем клиентом, который задаёт неудобные вопросы

Придя в Yandex Cloud

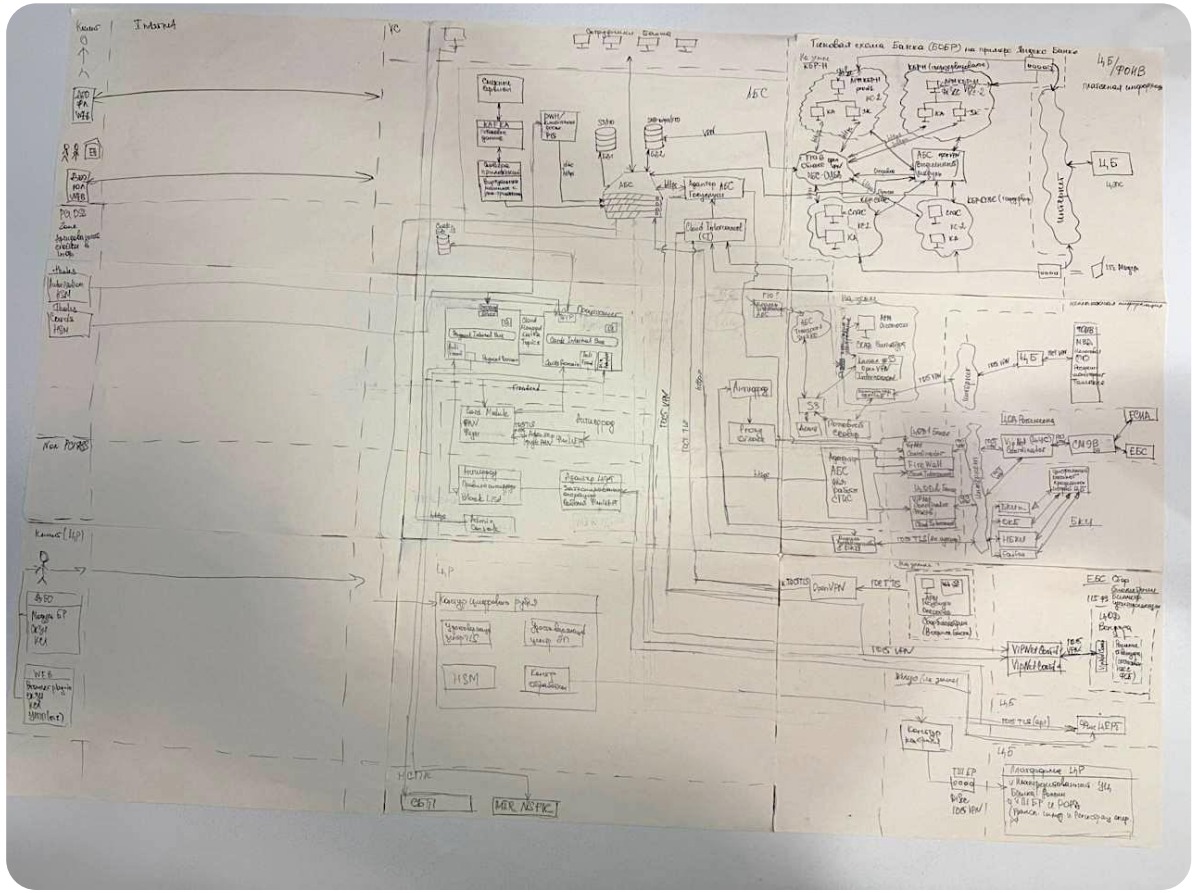
Я стал смотреть на облако с клиентской стороны: что на самом деле волнует того, кто решает – мигрировать в облако или нет?

Безопасник обычно говорит «нельзя»

Моя работа — перевести требование регулятора в меру, понятную ИТ и не сломать при этом бизнес

#PAYMENTSECURITY

Карта, с которой всё началось



Девять листов А4, карандаш, ластик и скотч. Карта архитектуры типового банка в облаке, нарисованная руками

Не дашборд и не красивая схема. Черновик, по которому виден весь путь: где переделывал, где соглашался, что было сырым.

Из этих листов выросло всё, что вы увидите дальше: типовая архитектура, фреймворк и схема ИБ, которые мы собрали командой

Зачем финтеху облако

#

Зачем финтеху облако

Курс ЦБ РФ на цифровизацию финансового сектора

Доступ к новым технологиям: ИИ и аналитика без сложных внедрений

Надёжность за счёт георезервирования дата-центров

Подтверждено: половина российского рынка облачных технологий — финансовый сектор*

* Согласно исследованию Б1, «Обзор рынка ИВНС и ПАК», апрель 2026 г.

#

Какие выгоды получает бизнес

Снижение затрат

Оплата по факту использования
вместо капитальных вложений в железо

Высокая скорость запуска продуктов

Новый сервис за дни,
а не месяцы

Повышение уровня ИБ

Экспертность провайдера закрывает
нехватку своих специалистов

Соответствие стандартам

152-ФЗ, ГОСТ Р 57580, PCI DSS,
ISO 27001

#

Почему именно сейчас

Платформы дозрели

Облако — уже не «экспериментальная» инфраструктура, на нём спокойно живут критичные системы

Появились нативные средства защиты

Сервисы ИБ, которых не было 3–5 лет назад, включаются кнопкой

Рынок движется к облачным моделям

Переезд — вопрос времени, а не вопрос выбора

Дословно, как говорят клиенты

Частые вопросы, которые задают клиенты

«Как я могу быть уверен, что ваш сотрудник не имеет доступа к моим ресурсам?»

Доступ к данным

«Используете ли вы мои данные для обучения своего ИИ»

Данные и ИИ

«Кто отвечает деньгами, если данные утекут?»

Ответственность

«ЦБ требует реагировать на инцидент за 24 часа. А за сколько реагируете вы?»

SLA по инцидентам

#

Мешают не технологии, а требования

Требования разбросаны по десятку документов, и ни один из них не написан про облако

Часть контроля над инфраструктурой уходит провайдеру — и это надо чем-то компенсировать

Перенос критичных систем — отдельный проект, а не «переключить рубильник»

Какой путь выбрать?

Продуктовый цикл	→	Конкурент выкатывает сервис за недели, пока вы ждёте поставку и монтаж железа
Кадры	→	Сильные инженеры уходят туда, где современный стек, и обратно не возвращаются
Капитал	→	Деньги заморожены в мощностях, которые загружены наполовину
Старт по закону об аутсорсинге	→	когда он заработает, готовым окажется тот, кто начал заранее — остальные встанут в очередь

Риск есть у обеих дверей. Вопрос не «идти ли», а на каких условиях вы приедете

Не документация, а готовый сценарий

Ответ на эти вопросы

Тип лицензии клиента

Банк | РНКО | ОФП | МФО | Платёжный агрегатор

Какие данные и какие требования применимы

- ДБО
- Мобильный и веб-банк
- Личные кабинеты клиентов

Сведение стандартов

- Маппинг требований, применимых к клиенту

Готовый чек-лист + архитектура

- Клиент получает дорожную карту, что и как ему нужно построить

Что меняется с введением закона об аутсорсинге

Отсутствие юридического статуса провайдера

Передача банковской тайны провайдеру и обязательные отдельные согласия субъектов на такую передачу

Отсутствие единых требований к поставщикам облачных услуг

Действуем в рамках текущего регулирования

Уже сегодня — и готовим клиентов к возможностям, которые откроет закон

Как мы подготовились

Готовый комплект артефактов для безопасного облачного банка:

- Типовая архитектура банка в облаке
- Фреймворк для самостоятельного использования
- Схема ИБ облачного банка
- Таблица соответствия требованиям регуляторов
- Матрица контролей выполнения требований
- Дорожная карта внедрения

#

Кому подходит и сколько занимает

Подходит всем компаниям финансового сектора

- Банки
- Страховые
- Инвестиционные компании
- МФО
- РНКО

Объём работ зависит от типа и количества мигрируемых систем — от аудита до полного внедрения

Ориентировочные сроки

- 1–3 месяца на пилот
- 3–9 месяцев на перенос боевых систем

Подход вендор-независимый

Открытые стандарты TOGAF и ArchiMate, применимы в любой облачной среде. Мы показываем его на своей реализации в Yandex Cloud

Шесть шагов, чтобы заехать

Шаг 1

Определить тип лицензии и бизнес-процессы

Шаг 2

Сегментировать системы:
что уходит в облако, что остаётся on-prem

Шаг 3

Собрать целевую архитектуру из референс-схем

Шаг 4

Смэпить применимые требования на контрольные меры

Шаг 5

Зафиксировать матрицу ответственности:
что закрывает провайдер, что финансовая организация

Шаг 6

Построить контур ИБ и подтвердить выполнение требований на аудите

Что чаще всего выносят в облако

Данные и аналитика

- Витрины и хранилища (DWH)
- BI
- Риск-аналитика
- Скоринг
- ИИ-ассистенты
- Чат-боты

Каналы и фронт

- ДБО
- Мобильный и веб-банк
- Личные кабинеты клиентов

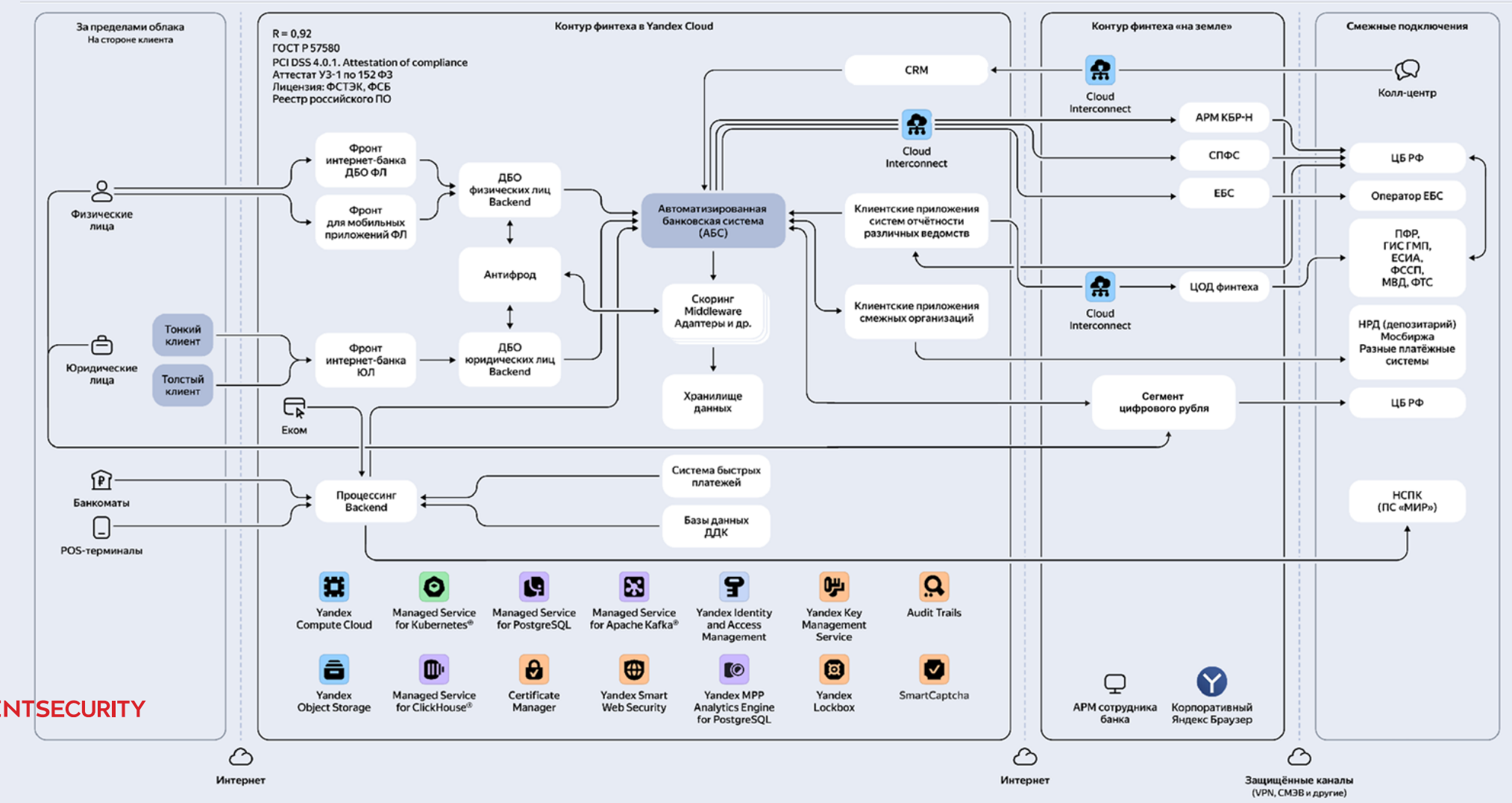
Безопасность и надёжность

- Контуры ИБ (SECaaS): SOC, SIEM, WAF, AntiDDoS, IAM
- Аварийное восстановление и резервирование (DR/BCP)

Разработка и офис

- Пайплайн безопасной разработки и DevSecOps под требования РБПО, среды dev/test
- Почта, CRM, документооборот, базы знаний

Общая схема безопасного облачного банка в Yandex Cloud



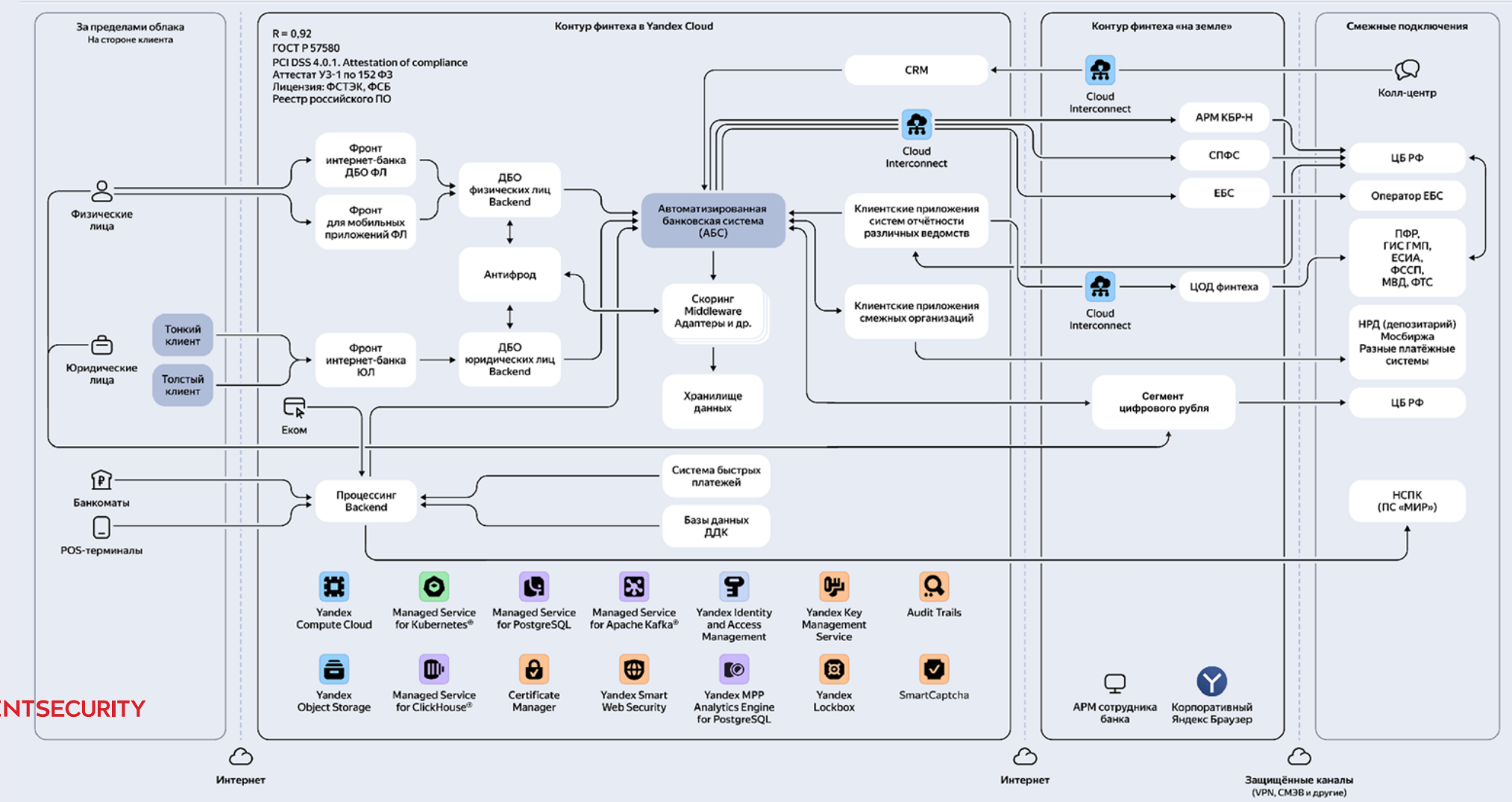
#PAYMENTSECURITY

#PAYMENTSECURITY

Типовая архитектура финтеха в облаке

Референсные архитектуры на открытых стандартах

Общая схема безопасного облачного банка в Yandex Cloud



#PAYMENTSECURITY

#

Как устроен фреймворк

Каталог референс-архитектур (TOGAF®, ArchiMate®, draw.io) с готовыми классами банковских систем

Клиент выбирает нужные системы и собирает из них целевую архитектуру

Схемы адаптируются под ландшафт, системы и требования конкретного банка

Архитектура проектируется не с нуля — референс-схемы используются как основа и конструктор, с индивидуальной адаптацией под клиента

#

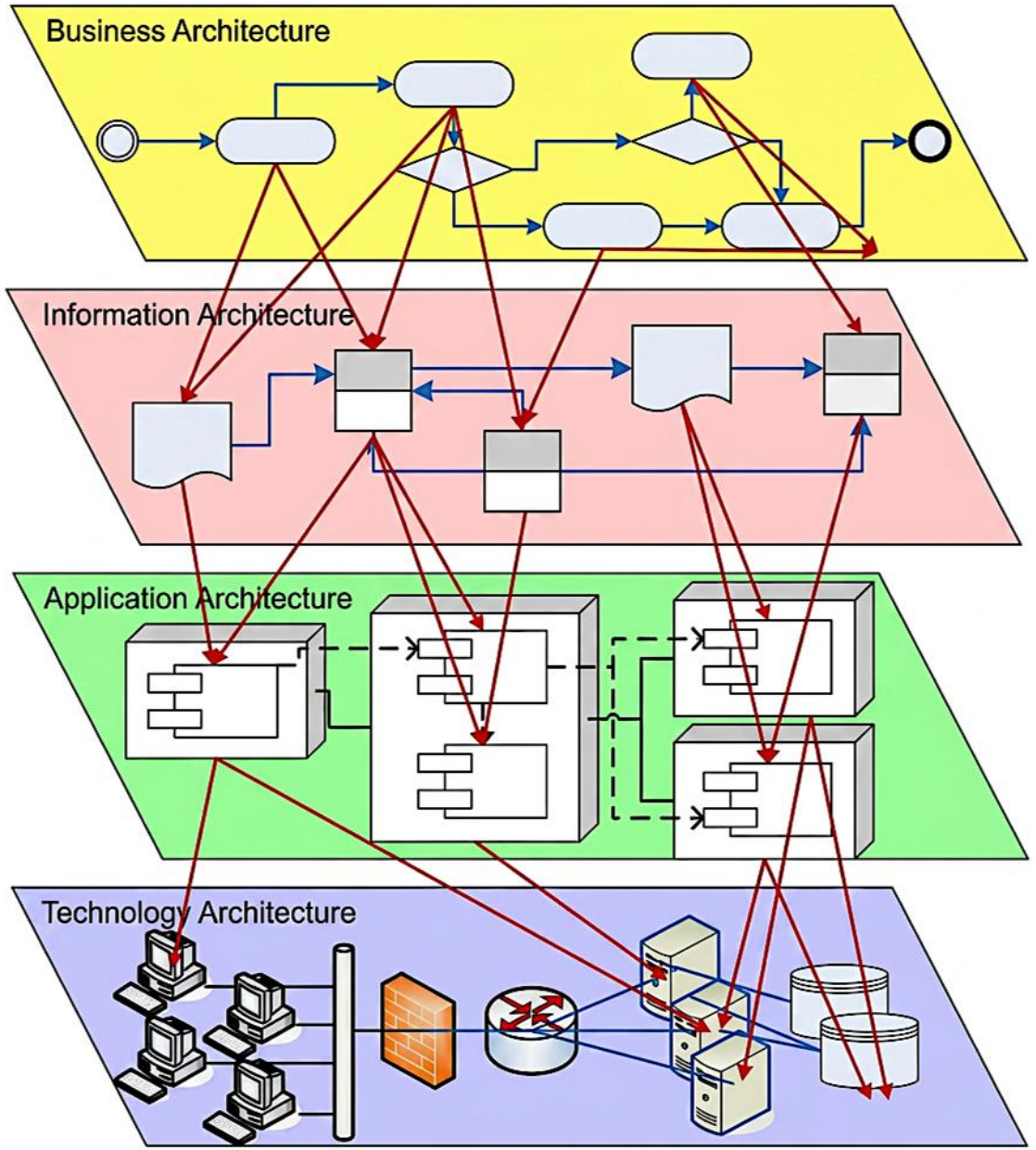
Стандарт TOGAF®

The Open Group Architecture Framework (TOGAF®) — признанный на международном и российском уровне фреймворк для проектирования и управления архитектурой корпоративной организации

Архитектурные уровни

- Уровень бизнес-архитектуры
- Уровень архитектуры данных
- Уровень архитектуры приложений
- Уровень технологической архитектуры

THE Open GROUP



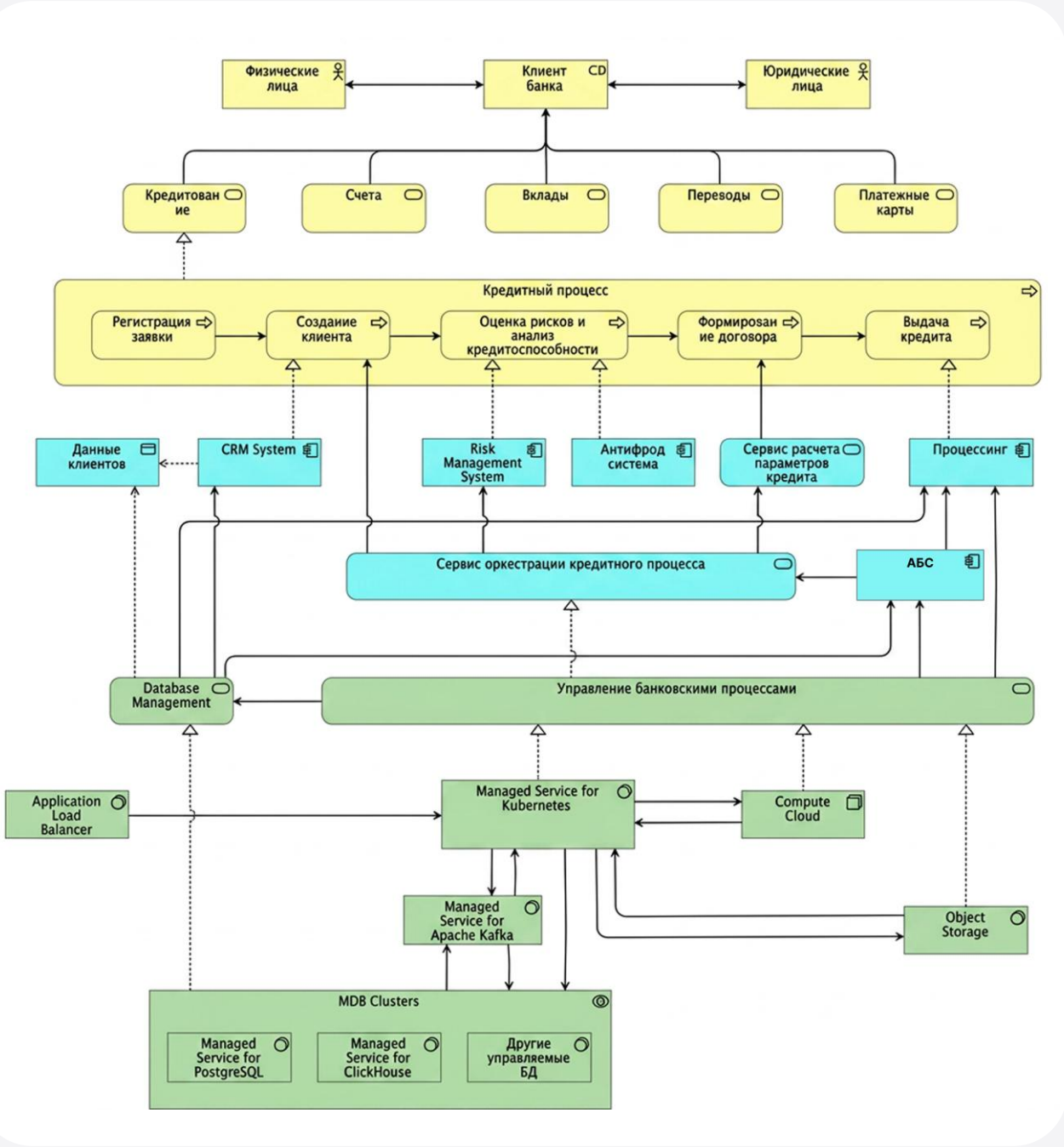
#PAYMENTSECURITY

#

Пример построения кредитного процесса

- Типовой банк спроектирован и представлен архитектурными уровнями в среде Archi®
- На данном примере представлена реализация кредитного процесса на уровне бизнес-архитектуры, архитектуры приложений и технологической архитектуры

Archi
archimate modelling



#PAYMENTSECURITY

#

Сценарии использования облаков финтехами

Уже в облаке

- Витрины данных и аналитика (DWH, BI, риск-аналитика)
- Фронтенд-каналы (ДБО, мобайл, веб-банк, ЛК)
- Контуры безопасности (SECaaS) – SOC, SIEM, WAF, AntiDDoS, IAM
- AI-платформа: скоринг, ИИ-ассистенты, чат-боты
- DR/BCP: резервирование и аварийное восстановление
- Пайплайн безопасной разработки и внедрение DevSecOps-практик
- Среда разработки и тестирования (dev/test)
- Офисные и вспомогательные сервисы (почта, CRM, таск-трекеры, базы знаний и документооборот)

Куда движется рынок
(единичные, не массовые реализации)

- Core-банкинг, АБС, скоринг, BaaS
- Платёжная инфраструктура и эквайринг (cloud native)
- KYC/AML/антифрод-платформы
- Автоматизация регуляторной отчетности и compliance как сервис

#PAYMENTSECURITY

Безопасность облачной инфраструктуры финтеха

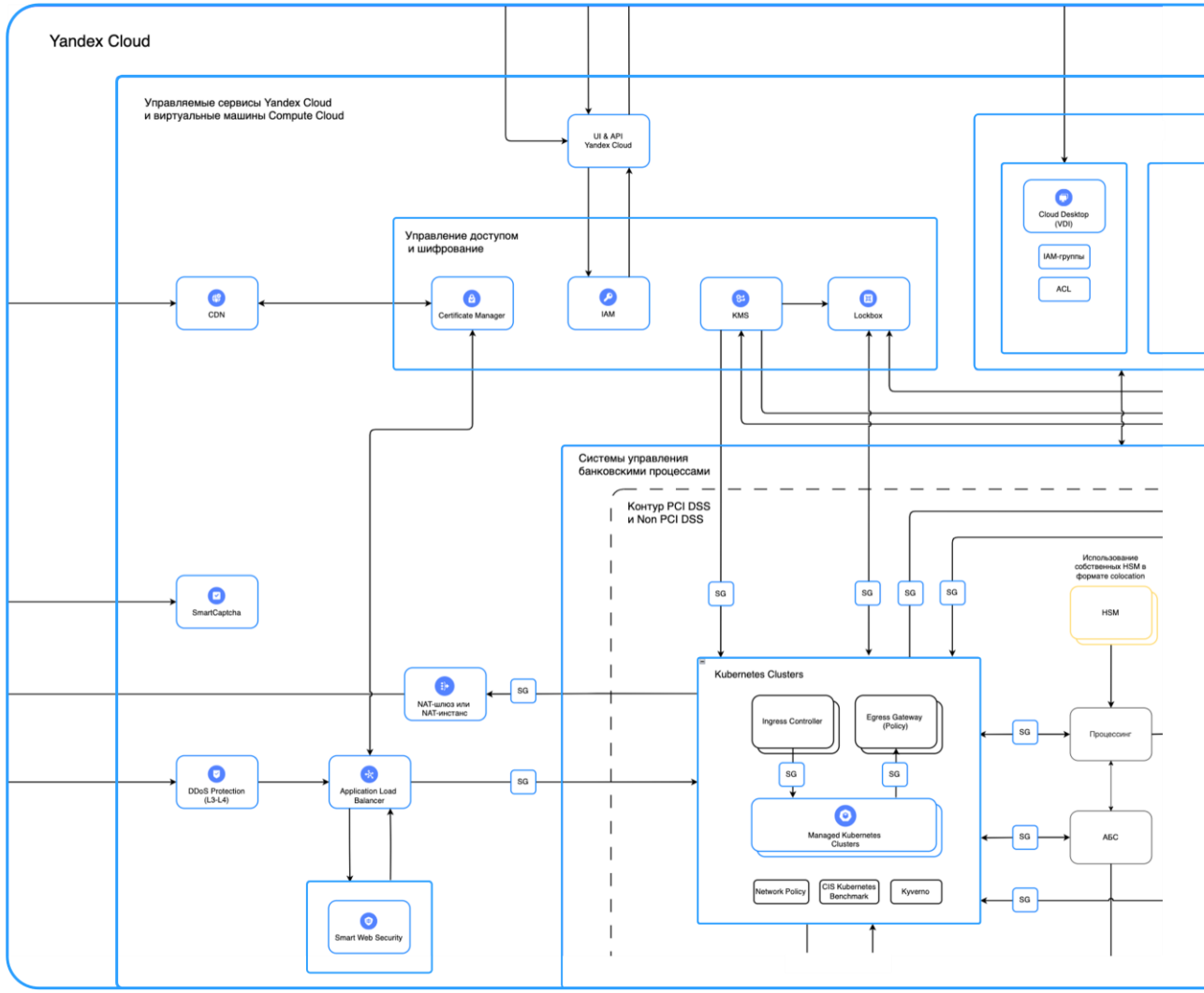
Схема информационной безопасности
и разделение ответственности

Схема ИБ облачного банка

Разработана схема обеспечения безопасности банковских информационных систем, реализованных в облачной инфраструктуре

Подготовлены:

- схема ИБ облачного банка на примере сервисов платформы Yandex Cloud
- описание схемы с рекомендациями по настройке инфраструктуры с учётом best practices
- описание взаимодействия среды on-premises и облачной инфраструктуры



#PAYMENTSECURITY

Описание схемы ИБ

- **Документ структурирован в соответствии с процессами обеспечения ИБ по ГОСТ Р 57580**
- **Детализированные схемы по каждому основному домену** Управление доступом, сетевая безопасность, мониторинг, сбор логов и т. д.
- **Приведены рекомендации по настройке инфраструктуры с учётом практик реальной ИБ и требований регуляторов**

#PAYMENTSECURITY

Описание схемы информационной безопасности облачного банка в инфраструктуре Yandex Cloud

Команда Yandex Cloud подготовила решение для кредитных и некредитных финансовых организаций (далее - финтех) с учетом практик реальной информационной безопасности и требований регуляторов, таких как, Банк России, ФСБ, ФСТЭК и НСПК.

Команда информационной безопасности Yandex Cloud подготовила материалы, необходимые для оценки и принятия решения о размещении финансовыми компаниями своей ИТ-инфраструктуры в облачной среде. В рамках данного проекта команда YC провела анализ и разработала схему ИБ банка в облачной инфраструктуре Yandex Cloud. На данной схеме отражены сервисы и инструменты безопасности, различные классы СЗИ и СКЗИ, необходимые любому финтеху для выполнения своих бизнес-функций, соответствующих лицензии финтеха.

Описание схемы ИБ

- **Документ структурирован в соответствии с процессами обеспечения ИБ по ГОСТ Р 57580**
- **Детализированные схемы по каждому основному домену** Управление доступом, сетевая безопасность, мониторинг, сбор логов и т. д.
- **Приведены рекомендации по настройке инфраструктуры с учётом практик реальной ИБ и требований регуляторов**

Процессы обеспечения информационной безопасности

1. Обеспечение защиты информации при управлении доступом
   - 1.1. Управление учетными записями и правами субъектов логического доступа
   - 1.2. Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа
   - 1.3. Защита информации при осуществлении физического доступа
   - 1.4. Идентификация, классификация и учет ресурсов и объектов доступа
2. Обеспечение защиты вычислительных сетей
   - 2.1. Сегментация и межсетевое экранирование вычислительных сетей
   - 2.2. Выявление сетевых вторжений и атак
   - 2.3. Защита информации, передаваемой по вычислительным сетям
   - 2.4. Защита беспроводных сетей
3. Контроль целостности и защищенности информационной инфраструктуры
4. Защита от вредоносного кода
5. Предотвращение утечек информации
6. Управление инцидентами защиты информации
   - 6.1. Мониторинг и анализ событий защиты информации
   - 6.2. Обнаружение инцидентов защиты информации и реагирование на них
7. Защита среды виртуализации
8. Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств
9. Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений
   - 9.1. На этапе «создания (модернизации) АС»
   - 9.2. На этапе «ввода в эксплуатацию АС»

Описание схемы ИБ

- **Документ структурирован в соответствии с процессами обеспечения ИБ по ГОСТ Р 57580**
- **Детализированные схемы по каждому основному домену** Управление доступом, сетевая безопасность, мониторинг, сбор логов и т. д.
- **Приведены рекомендации по настройке инфраструктуры с учётом практик реальной ИБ и требований регуляторов**

#PAYMENTSECURITY

В Yandex Cloud есть два способа построения корпоративной системы Single Sign-On (SSO) в организации

1. Использовать Yandex Identity Hub в качестве IdP-сервиса
2. Использовать собственный IdP-сервис

Схема 1. Yandex Identity Hub в качестве IdP-сервиса

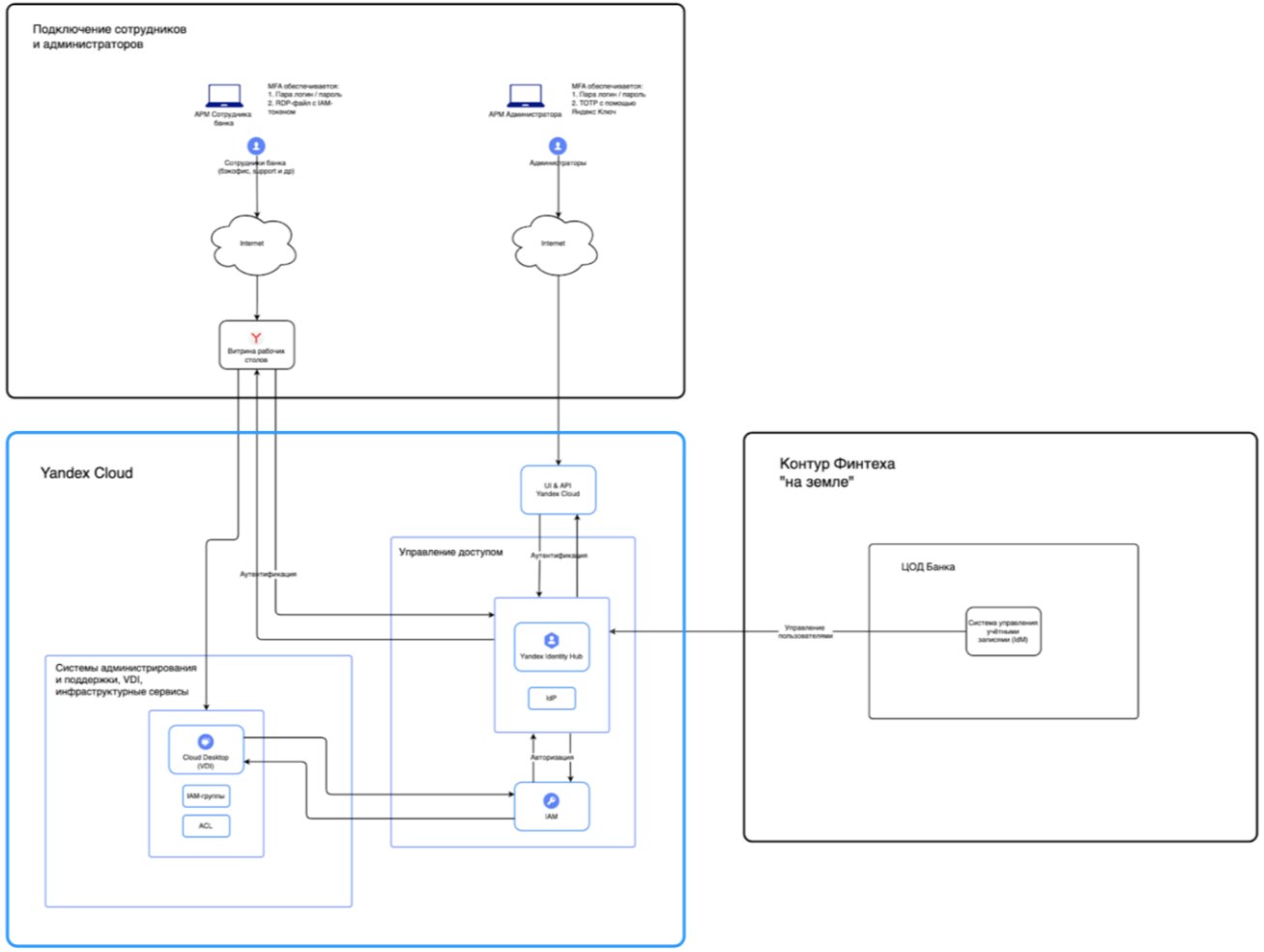


Схема 1. Управления учетными записями и правами субъектов логического доступа с использованием Yandex Identity Hub в качестве IdP-сервиса

#

Соответствие требованиям регуляторов

Подготовлено соответствие используемых в облачной инфраструктуре средств и инструментов ИБ требованиям регуляторов для финтеха (ГОСТ Р 57580, PCI DSS, Приказ ФСТЭК 21, Положения Банка России № 851-П, 802-П, 821-П)

Стандарт	ГОСТ Р 57580.1-2017
Название требования	УЗП.1
Содержание требования	Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями
Тип требования	Техническое
Реализация в Yandex Cloud	Права назначаются через роли, привязанные к группам (например, employees, contractors, admins), а не к отдельным пользователям. Сотрудники работают только под персональными учётными записями, сервисные обращения — через service accounts или федерации сервисных аккаунтов
Сервисы и инструменты Yandex Cloud	Identity Hub, Identity and Access Management, Audit Trails, Security Deck, Yandex Cloud Detection and Response
Внешние инструменты	IdM, IdP, AD

Взаимодействие облака и on-prem

Гибридная инфраструктура давно стала нормой — с единым контуром безопасности

Сеть и отказоустойчивость

- Основной канал – Cloud Interconnect, резервный – VPN (IPsec/WireGuard)
- BGP: автопереключение при отказе канала
- Мониторинг качества каналов
- Мультизональность: критичные сервисы – минимум в двух зонах доступности
- Автомасштабирование и балансировка нагрузки (ALB) с health-checks

1

Сбор событий ИБ

- События из облака и on-prem собираются в один таймлайн
- Audit Trails: Control Plane включен по умолчанию, Data Plane – требует явного включения
- Корреляция разрозненных событий в единый инцидент
- Использовать YCDR — управляемый облачный SOC (MDR/SOCaaS)
- Или экспорт журналов и алертов во внешний SOC/SIEM банка

2

Взаимодействие облака и on-prem

Гибридная инфраструктура давно стала нормой — с единым контуром безопасности

Репликация и восстановление данных

- Репликация между зонами внутри облака
- Критичные транзакционные сервисы – синхронная репликация
- Бизнес-системы, системы поддержки и вспомогательные системы – асинхронная репликация
- Регулярное резервное копирование критичных данных
- Хранение бэкапов в географически разнесённых хранилищах

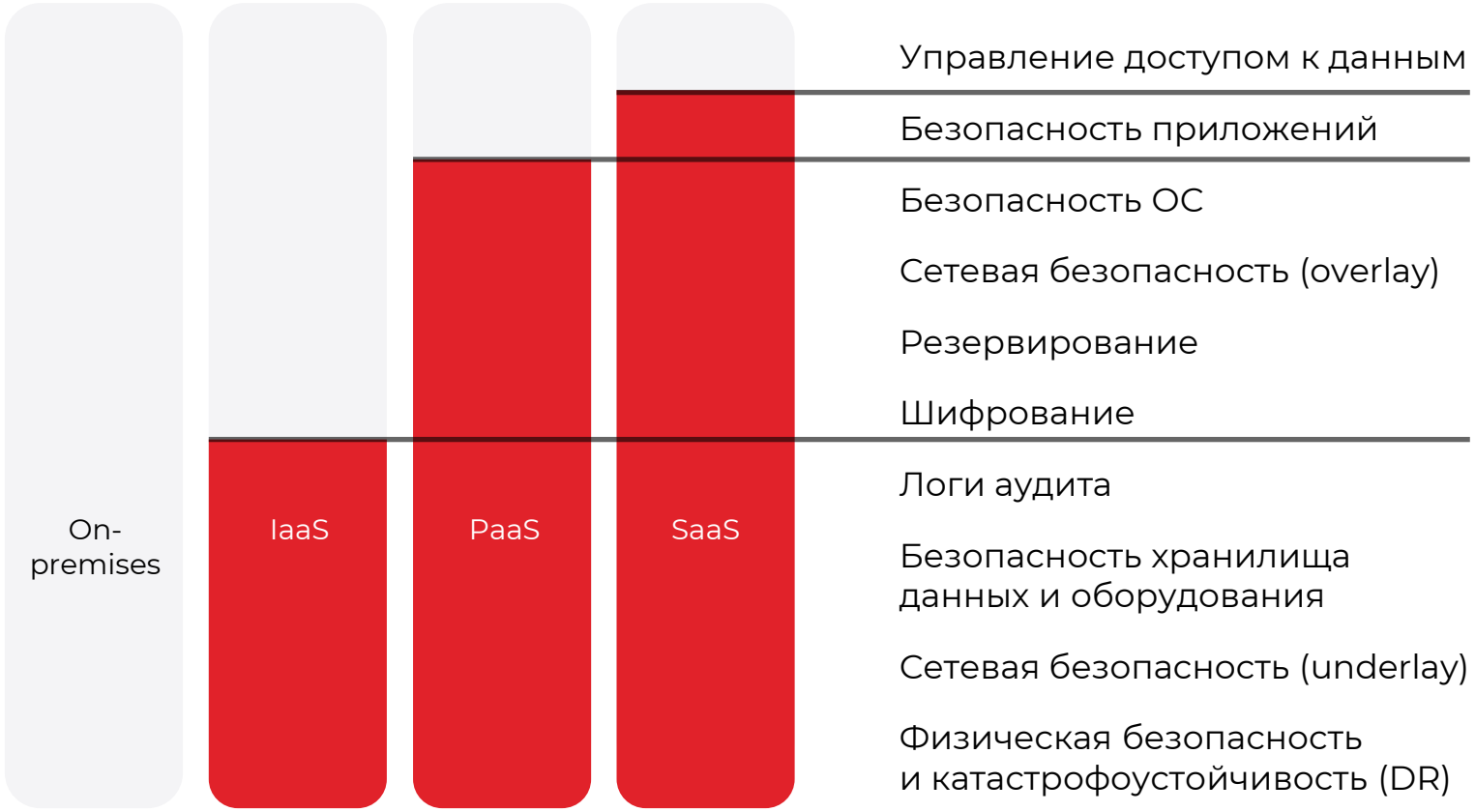
3

Мониторинг инфраструктуры

- Непрерывный контроль CPU, сети, доступности сервисов
- Отправка метрик из on-prem инфраструктуры в Yandex Monitoring
- Или экспорт метрик во внешние системы (Prometheus, VictoriaMetrics, Grafana)
- Централизованная система мониторинга для гибридной инфраструктуры

4

Совместная ответственность облака и клиента



- Ответственность клиента
- Ответственность Yandex Cloud

#PAYMENTSECURITY

#PAYMENTSECURITY

Как требования превращаются в технические контроли

От строчки в стандарте
до автоматической проверки

Матрица контролей выполнения требований

Требование → кто закрывает → чем закрывается → подтверждение выполнения

Часть требований банк «наследует» от платформы — уже закрыто на уровне облака

В интерфейсе Security Deck с автоматическим отслеживанием статуса и в формате документации

Автоконтроли разрабатываются постоянно, покрытие требований растёт

#

От требования к техническому контролю

Требование ГОСТ Р 57580

УЗП.1. Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учётными записями

Инструкция и рекомендации

Права назначаются через роли, привязанные к группам (например, employees, contractors, admins), а не к отдельным пользователям. Сотрудники работают только под персональными учётными записями, сервисные обращения — через service accounts или федерации сервисных аккаунтов

Сервисы

Yandex Identity Hub

Yandex Identity and Access Management

Audit Trails

Security Deck

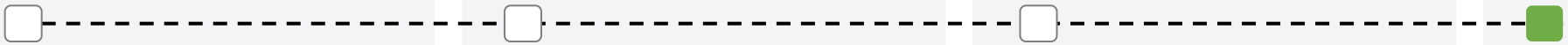
Yandex Cloud Detection and Response

Контроль

Контроль использования Яндекс ID (cspm.yandex-id-accounts)

Учёт сервисных аккаунтов (cspm.sa)

Создание/обновление SAML-федерации (audittrail/CreateFederation)



#

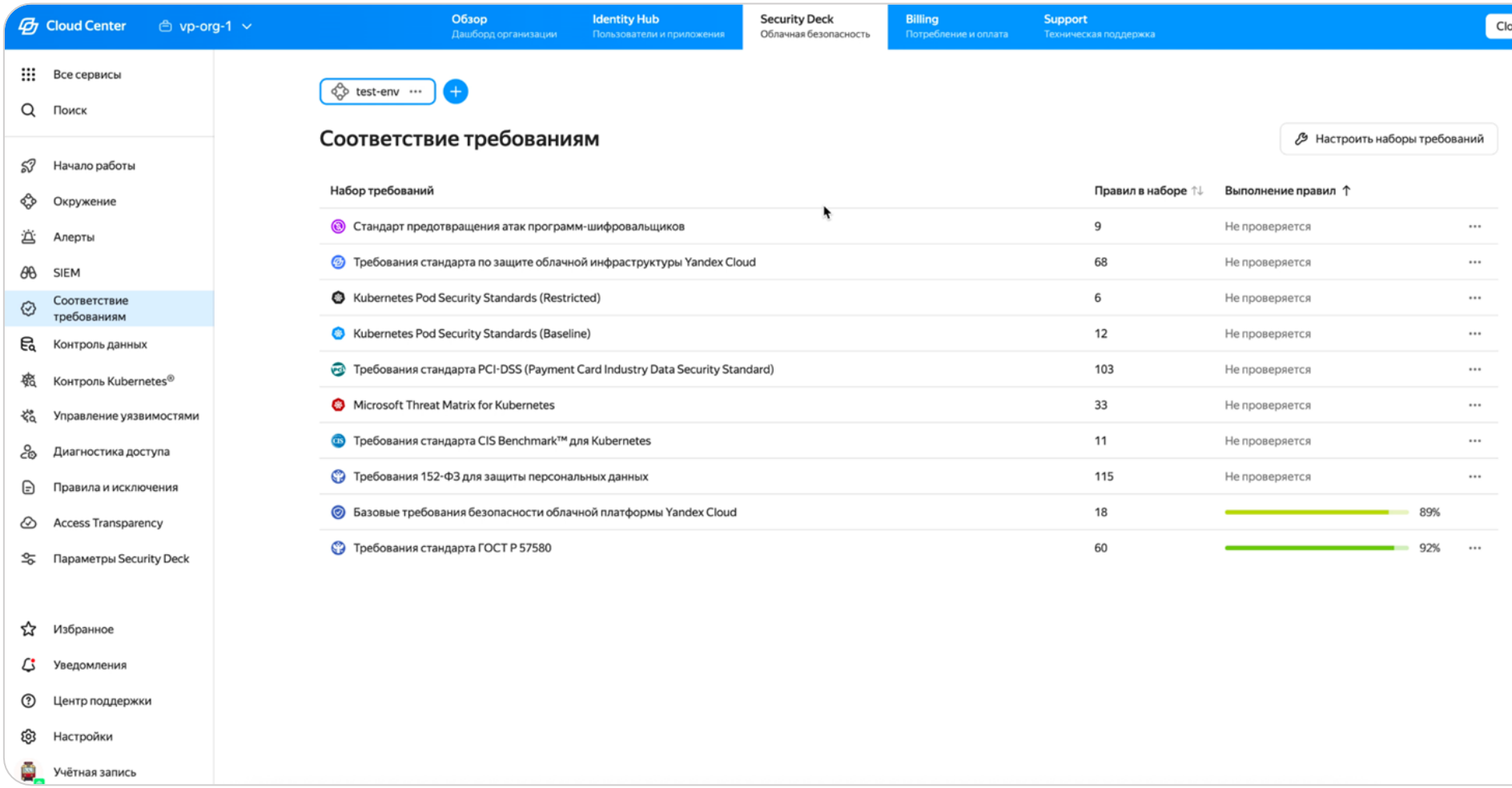
Практическая реализация

1.

Создаем окружение, которое хотим контролировать

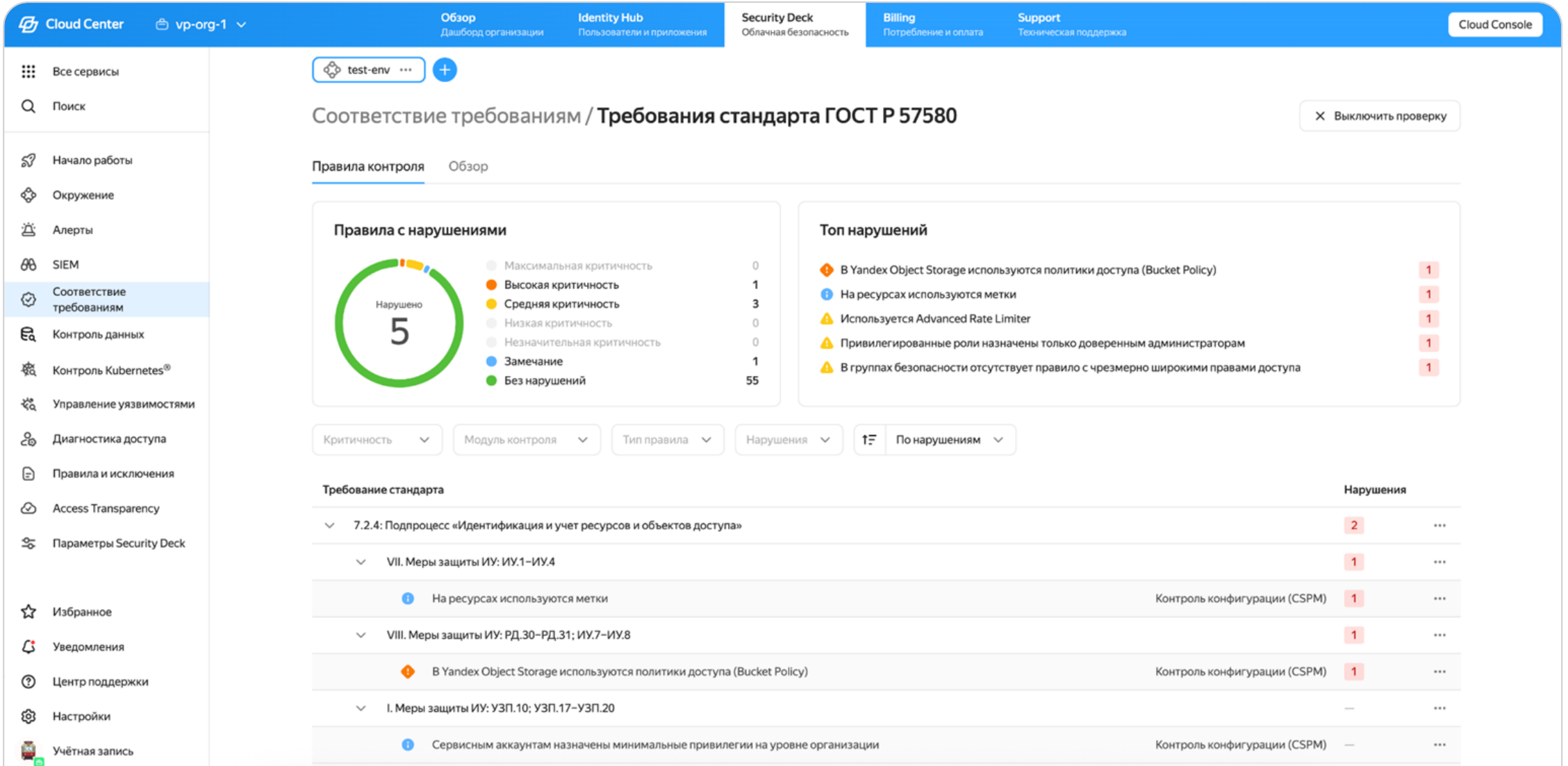
2.

Выбираем требования, которым должна соответствовать облачная инфраструктура

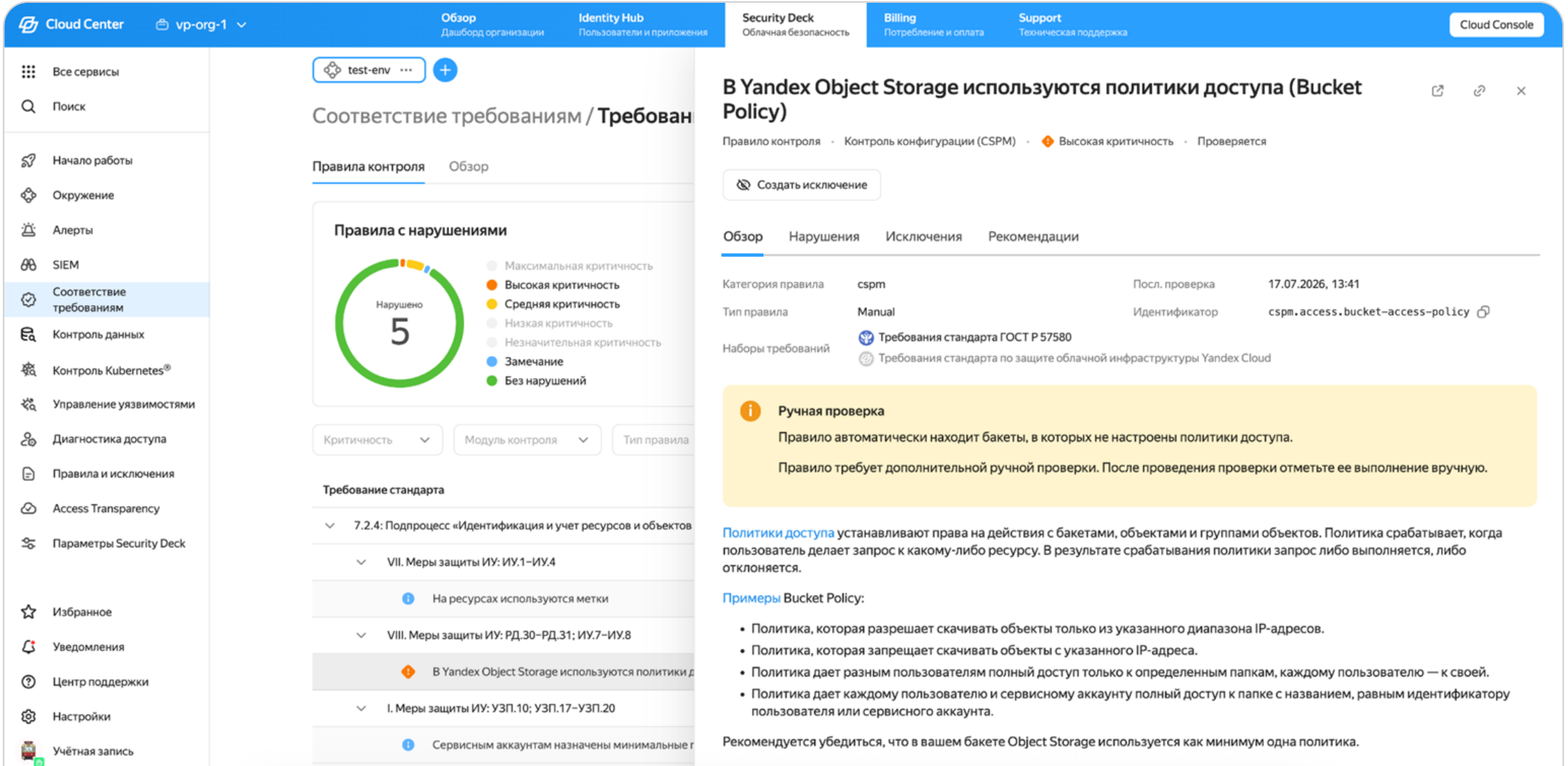


#PAYMENTSECURITY

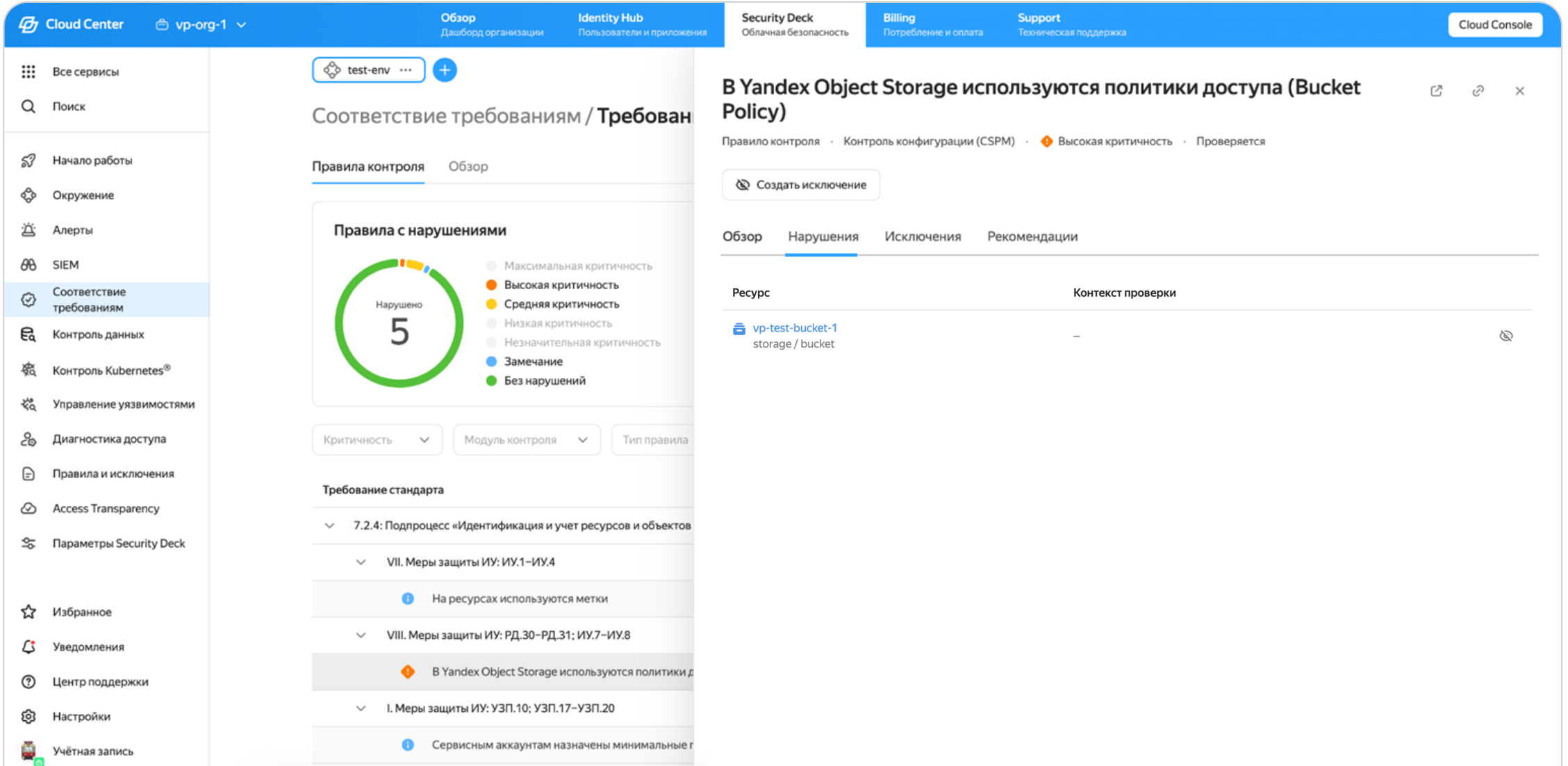
Дашборд соответствия ГОСТ Р 57580



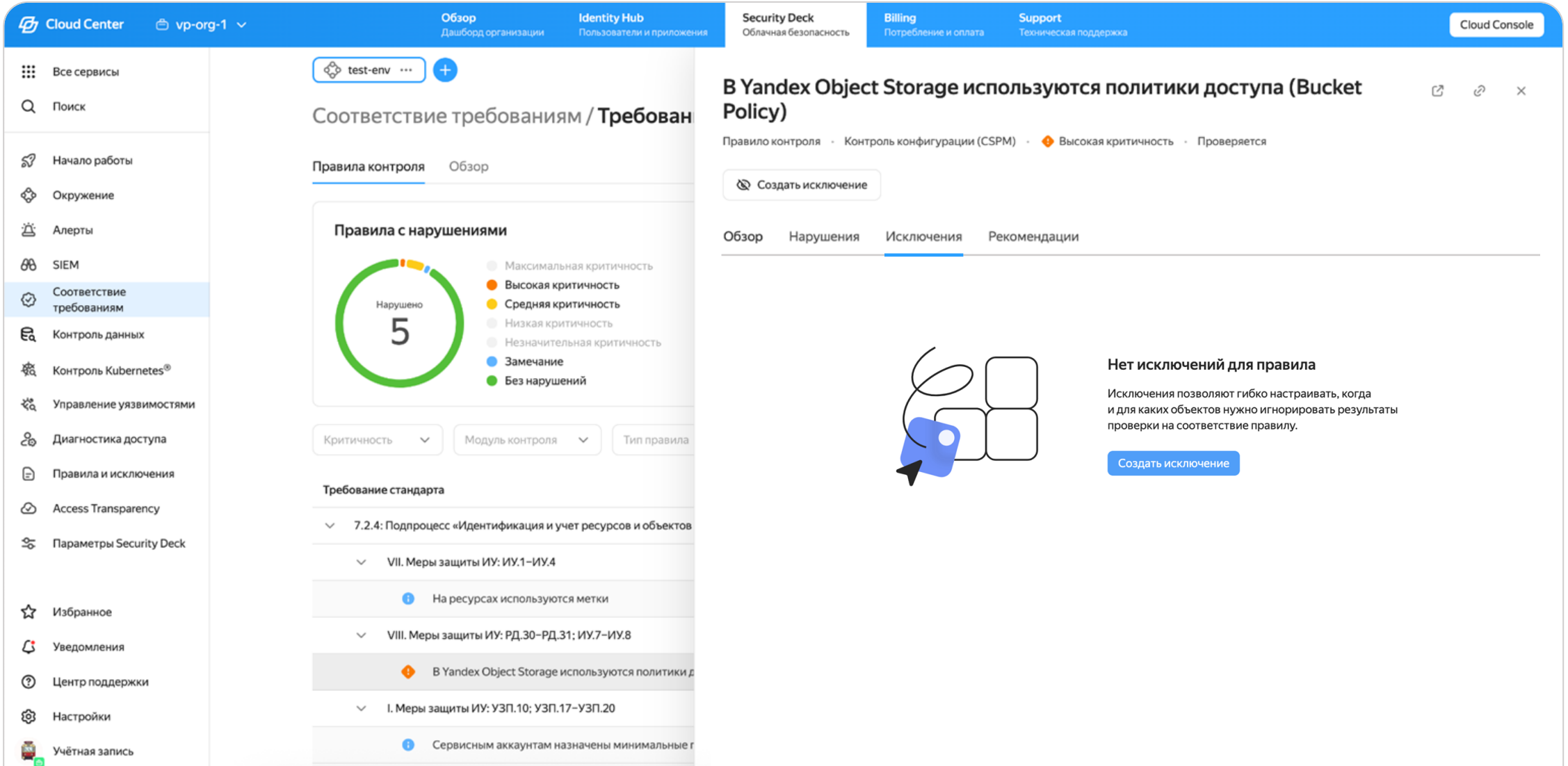
Нарушение с высоким уровнем критичности



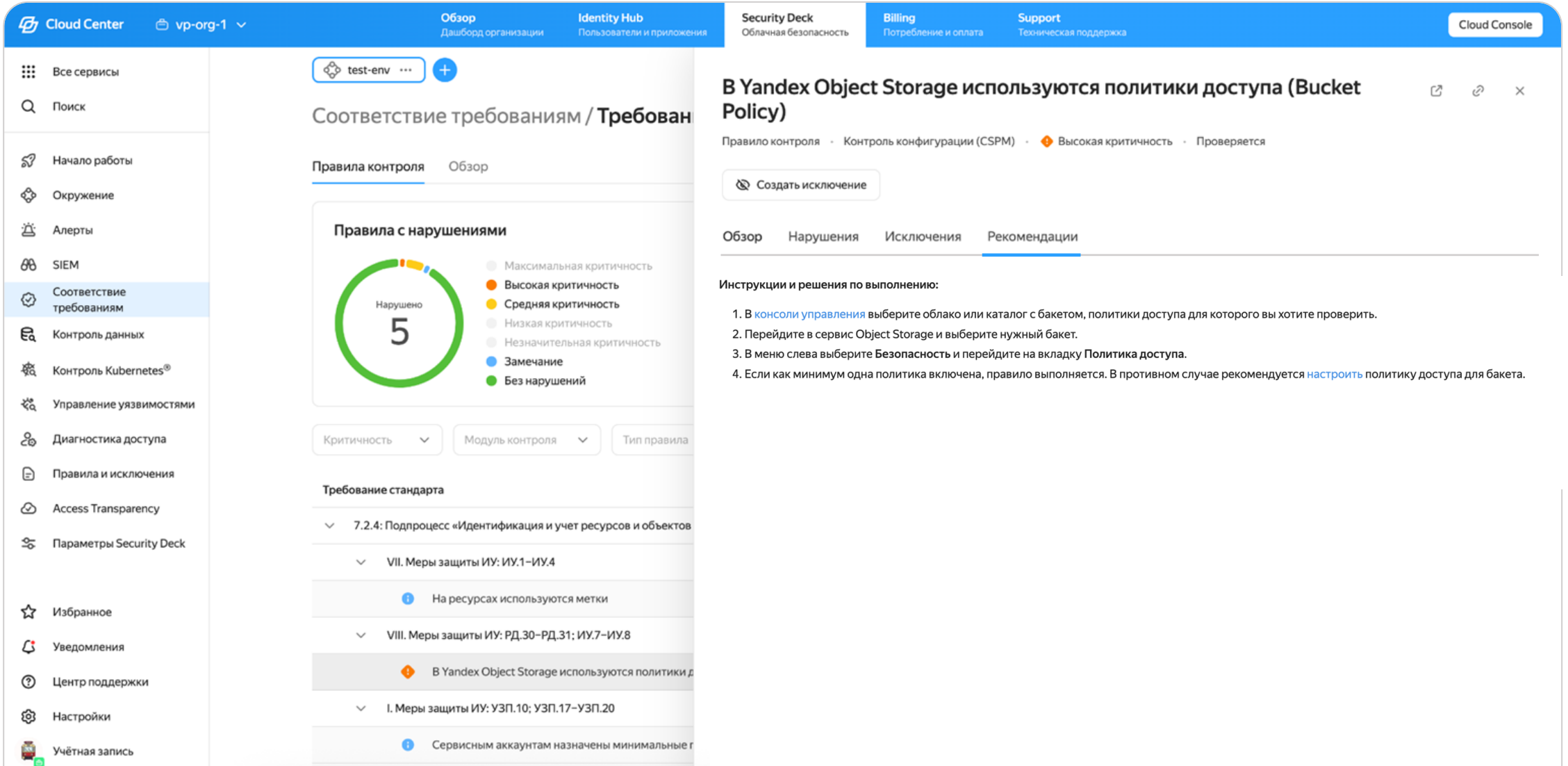
Нарушение с высоким уровнем критичности



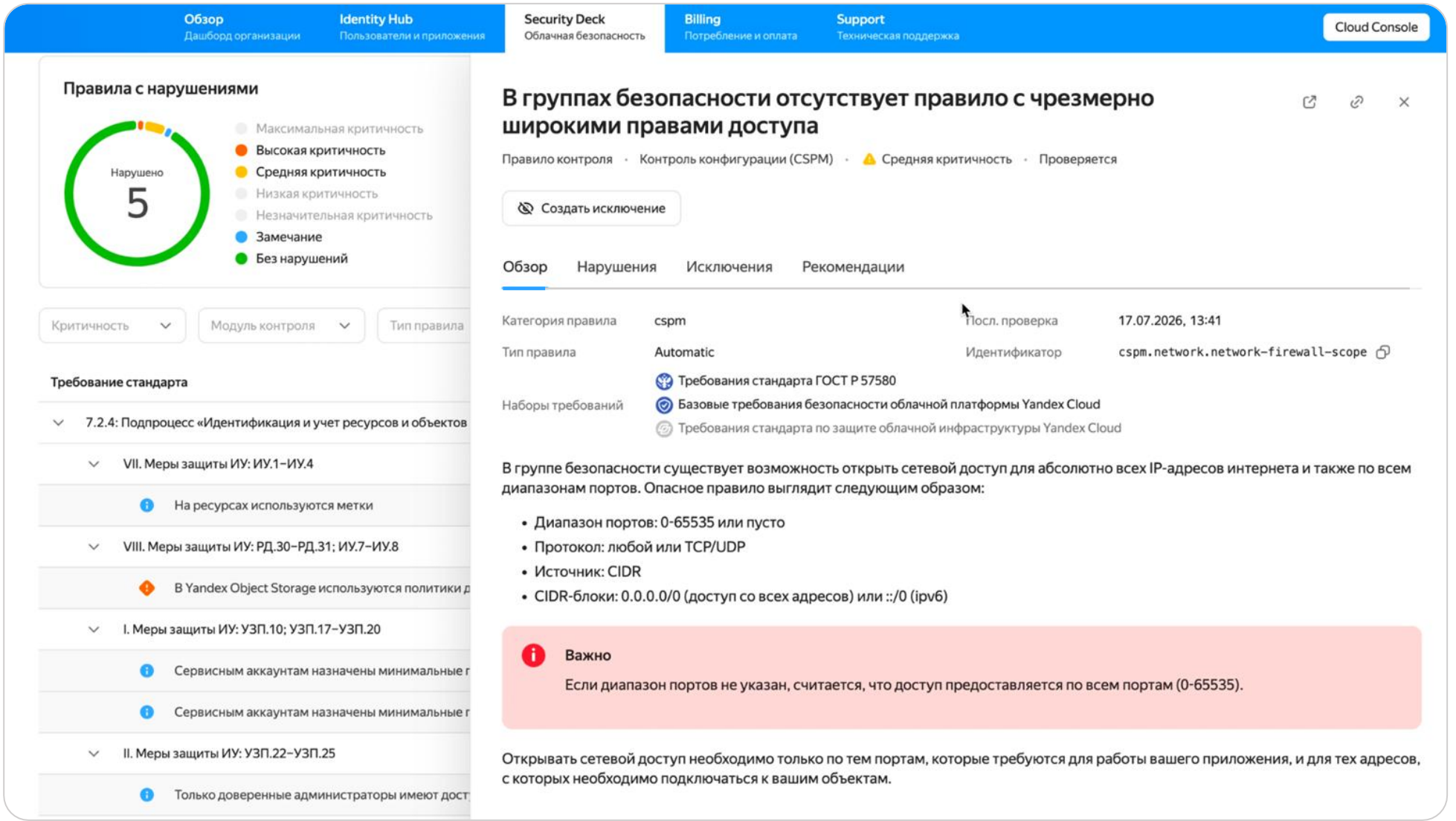
Нарушение с высоким уровнем критичности



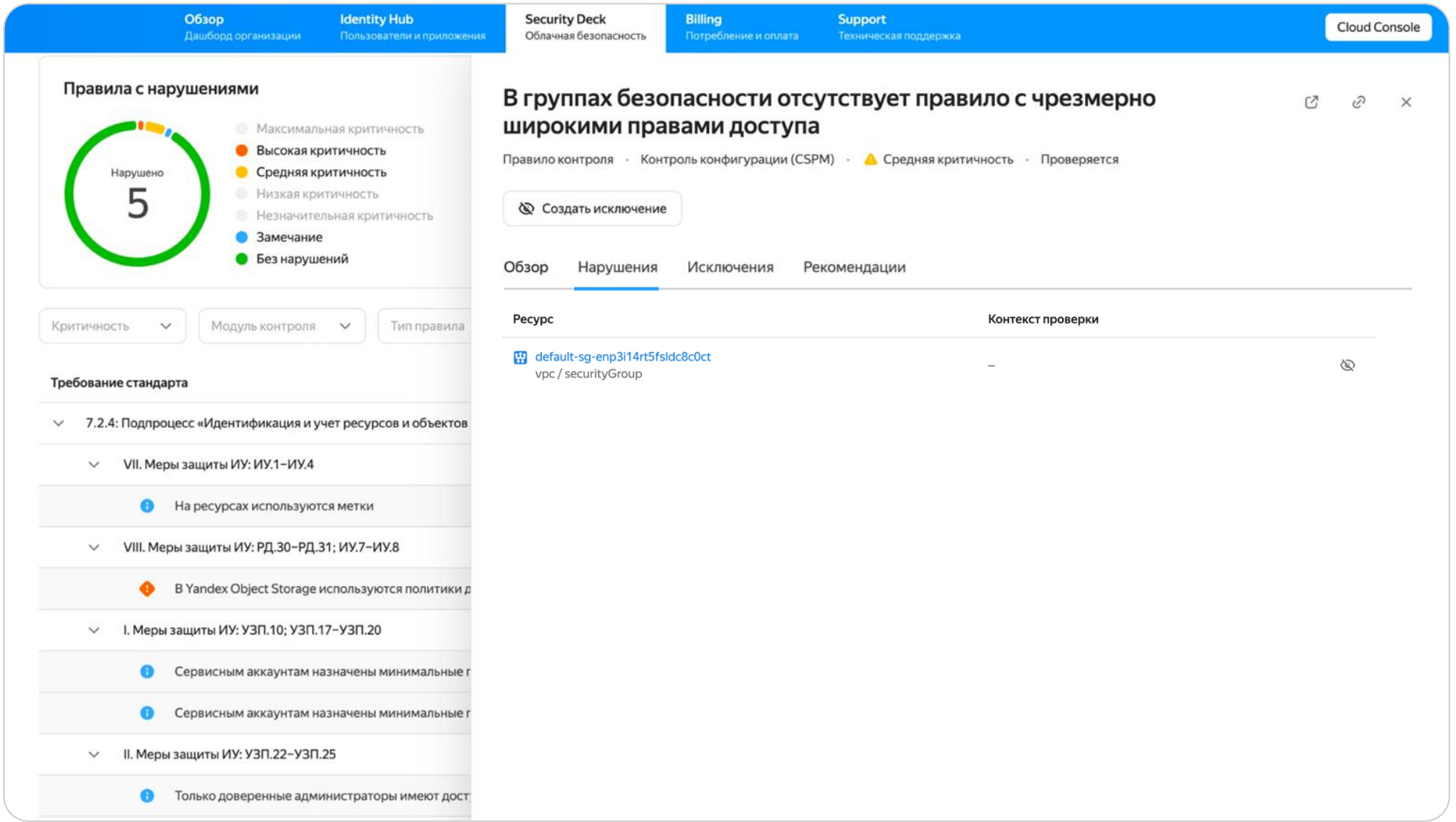
Нарушение с высоким уровнем критичности



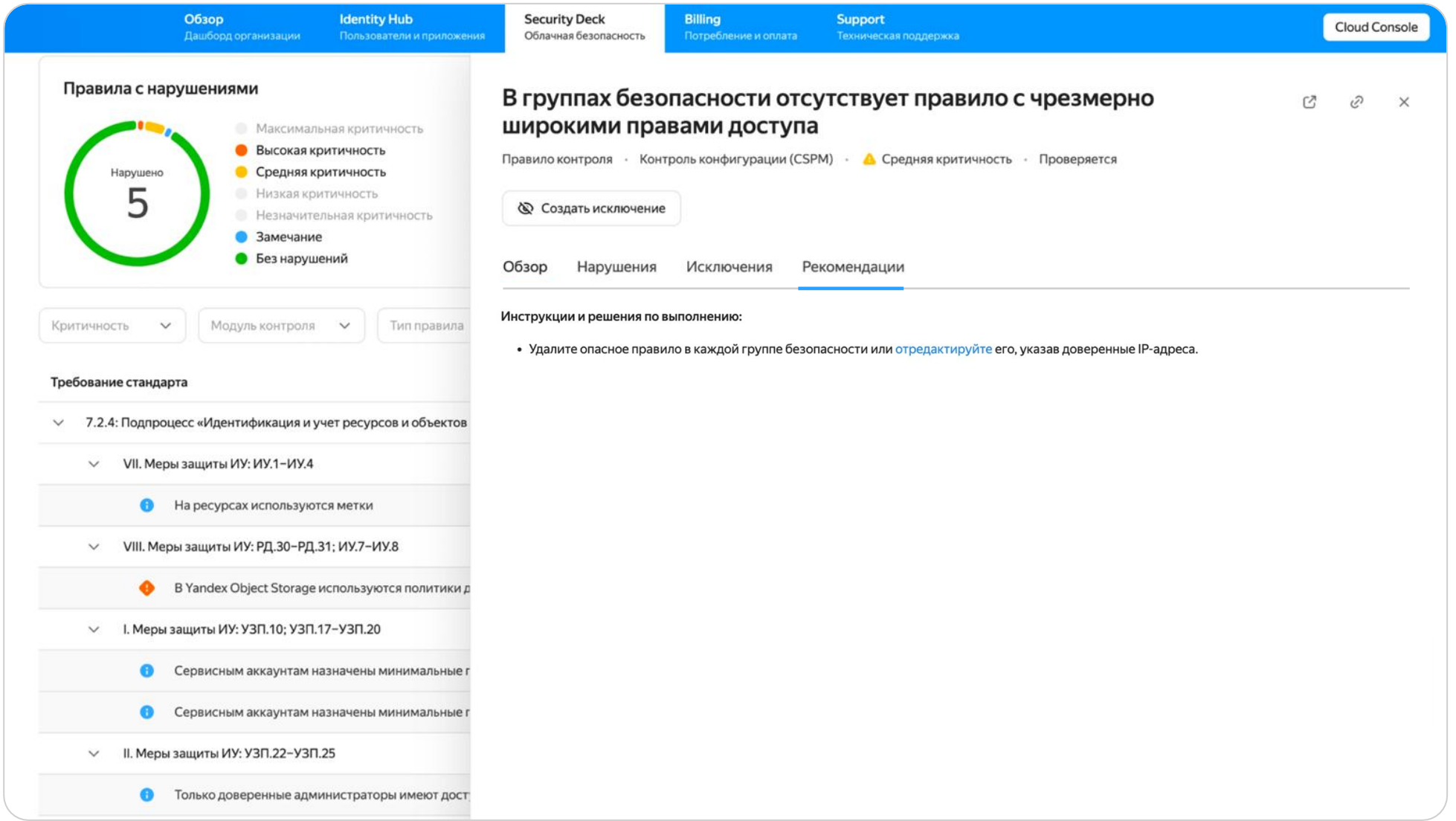
Использование групп безопасности с широкими правами доступа



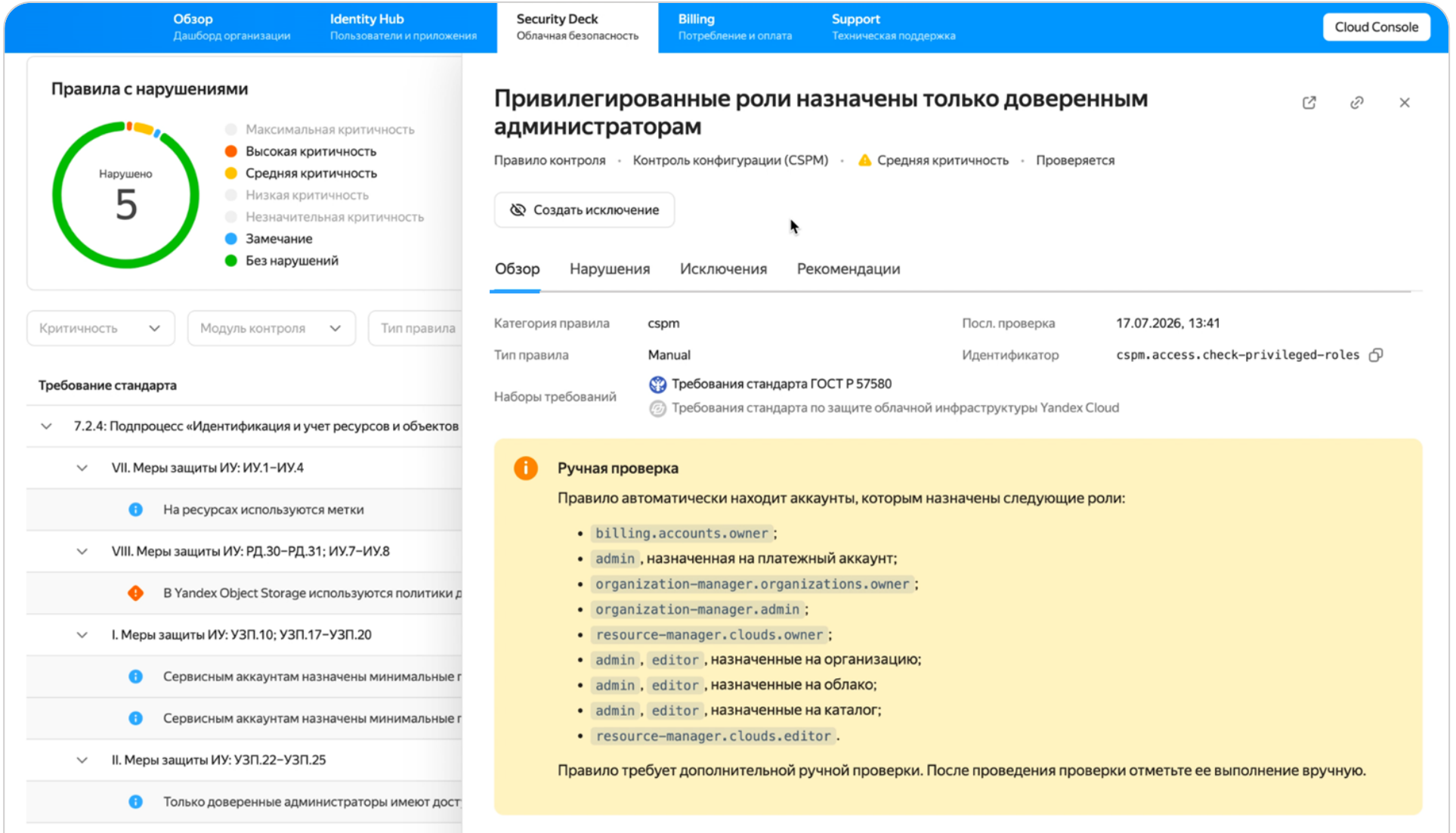
Использование групп безопасности с широкими правами доступа



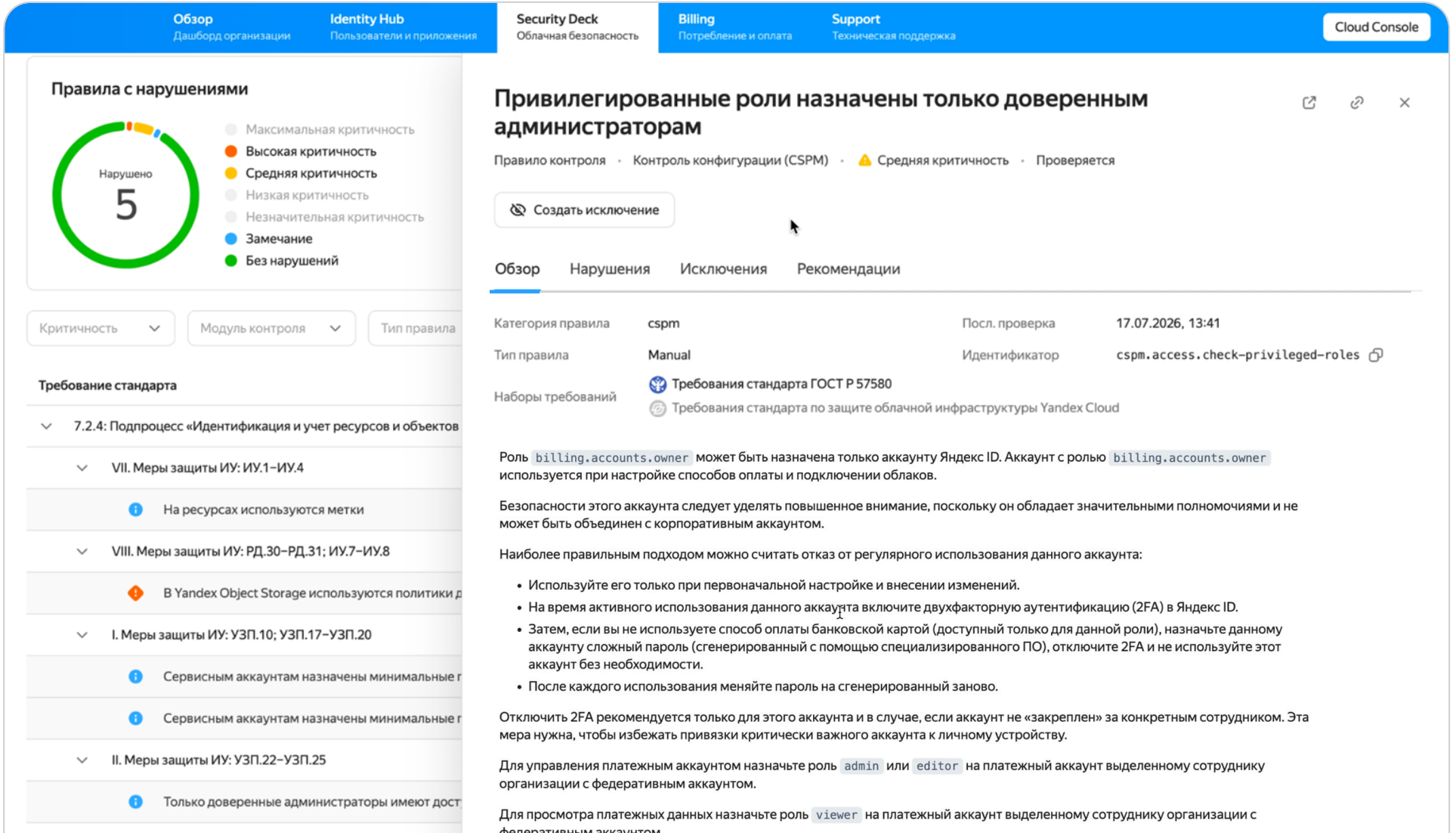
Использование групп безопасности с широкими правами доступа



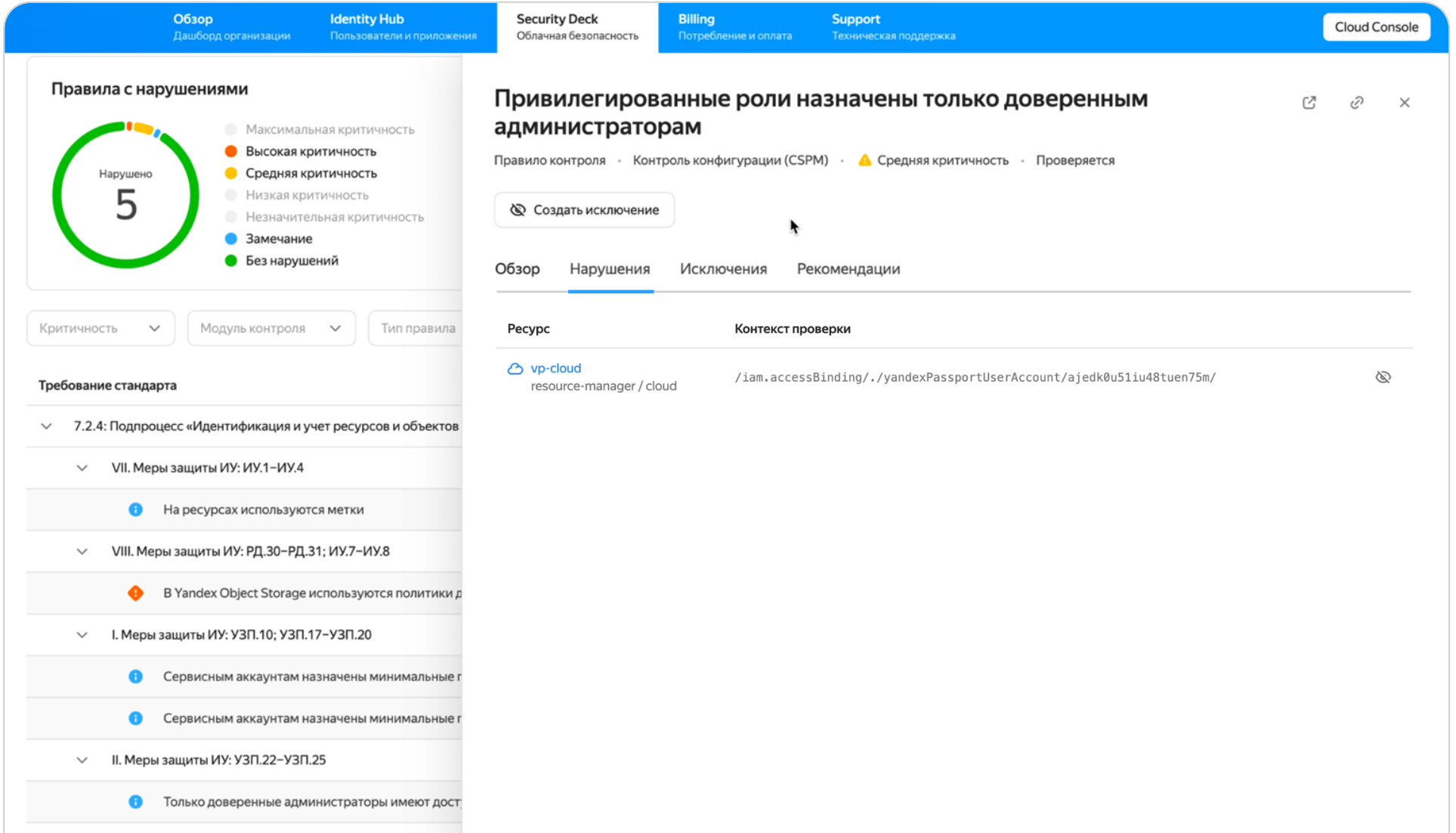
Назначение привилегированных ролей только доверенным администраторам



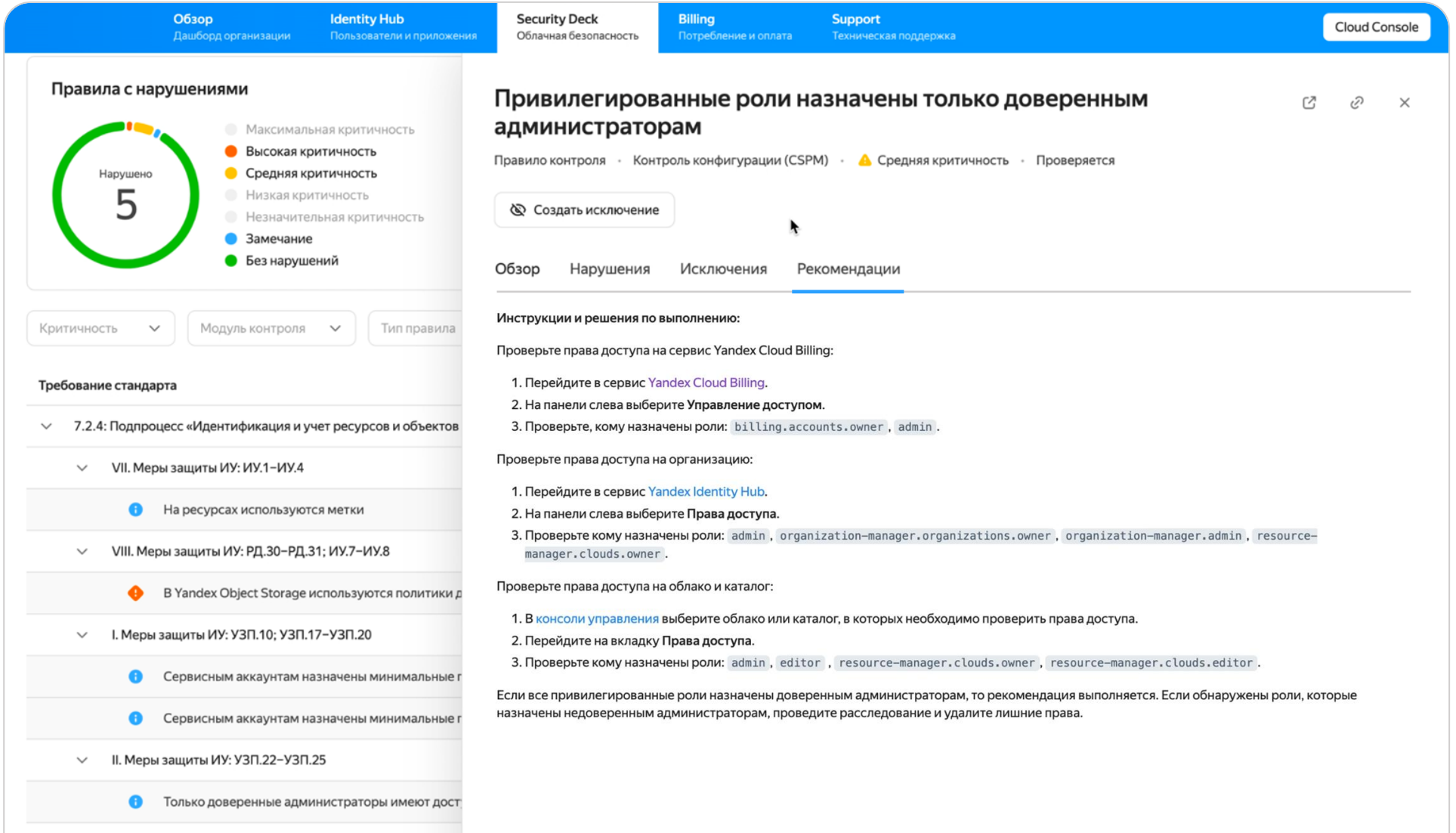
Назначение привилегированных ролей только доверенным администраторам



Назначение привилегированных ролей только доверенным администраторам



Назначение привилегированных ролей только доверенным администраторам



#

Что мы разобрали

Архитектура

Конструктор из референс-схем на открытых стандартах, который адаптируется под задачи клиента

Безопасность

Спроектирована с учетом требований стандартов, с чётким разделением ответственности между облаком и клиентом

Практика

Проверка выполнения требований с помощью автоматических и ручных контролей

КЕЙС

АО «Финсделка» вошла в реестр ОФП Банка России, находясь в Yandex Cloud

- Своя инфраструктура — это 70–100 млн рублей капитала и месяцы на поставку оборудования
- Компания развернула инфраструктуру в Облаке с нуля
- Сократили время запуска и оптимизировали стоимость всего проекта

- Выполнили требования 742-П
- Прошли оценку соответствия по ГОСТ Р 57580.1-2017
- Вошли в реестр операторов финансовых платформ. Пять месяцев, без единой закупленной стойки

Сопровождение на каждом шаге

От целевой архитектуры до подтверждения соответствия

#PAYMENTSECURITY

Дорожная карта внедрения

Этап 1

Анализ текущего состояния

Отчёт об аудите IT-инфраструктуры

Заполненный детальный шаблон соответствия требованиям регуляторов

Матрица рисков

Этап 2

Проектирование архитектуры

Архитектурные схемы уровней бизнеса, приложений, данных и технологической архитектуры

Итоговая сетевая схема

Итоговая схема ИБ

Детальный план миграции

Этап 3

Пилот, миграция и тестирование

Программа и методика испытаний

Отчёт по пилоту

Отчёт о функциональном и нагрузочном тестировании

Отчёт о тестировании безопасности

Этап 4

Запуск и сопровождение

Комплект эксплуатационной документации

Адаптированная программа обучения

Рекомендации по оптимизации архитектуры и затрат

План развития инфраструктуры

Этап 5

Прохождение аудита

Отчёт о тестировании безопасности и соответствии требованиям регуляторов

Заключение о соответствии, аттестат соответствия

#

С чего начать

01

Оцените свою готовность

02

Узнать больше про Cloud Trust

03

Нужна помощь?

#PAYMENTSECURITY

#PAYMENTSECURITY

Александр Мизерин

Эксперт по информационной безопасности,
Yandex Cloud

mizerinas@yandex-team.ru

Василий Пургин

Архитектор решений,
Affirmative Systems

vp@affirmative.pro

Спасибо за внимание!

#PAYMENTSECURITY

Вопросы?