

# ГОСТ 57580 В «РЕАЛЬНОМ» ВРЕМЕНИ

Департамент  
развития бизнеса

Открываем  
новый  
филиал!

Грядет  
проверка ЦБ

Мы нашли в  
Интернете клон  
нашего сайта

Пришли новые  
индикаторы и,  
похоже, есть  
сработки

СВК

Увольняется  
админ!

А мы внедряем  
новую фичу в  
АБС!

PR

SOC

Госдума утвердила  
поправки в 152-ФЗ, а  
ЦБ выпустило новое  
положение

Юристы

Переходим на  
новое сетевое  
оборудование  
и провайдера  
меняем!

Админы

Кадры

Программисты

Проектный  
офис

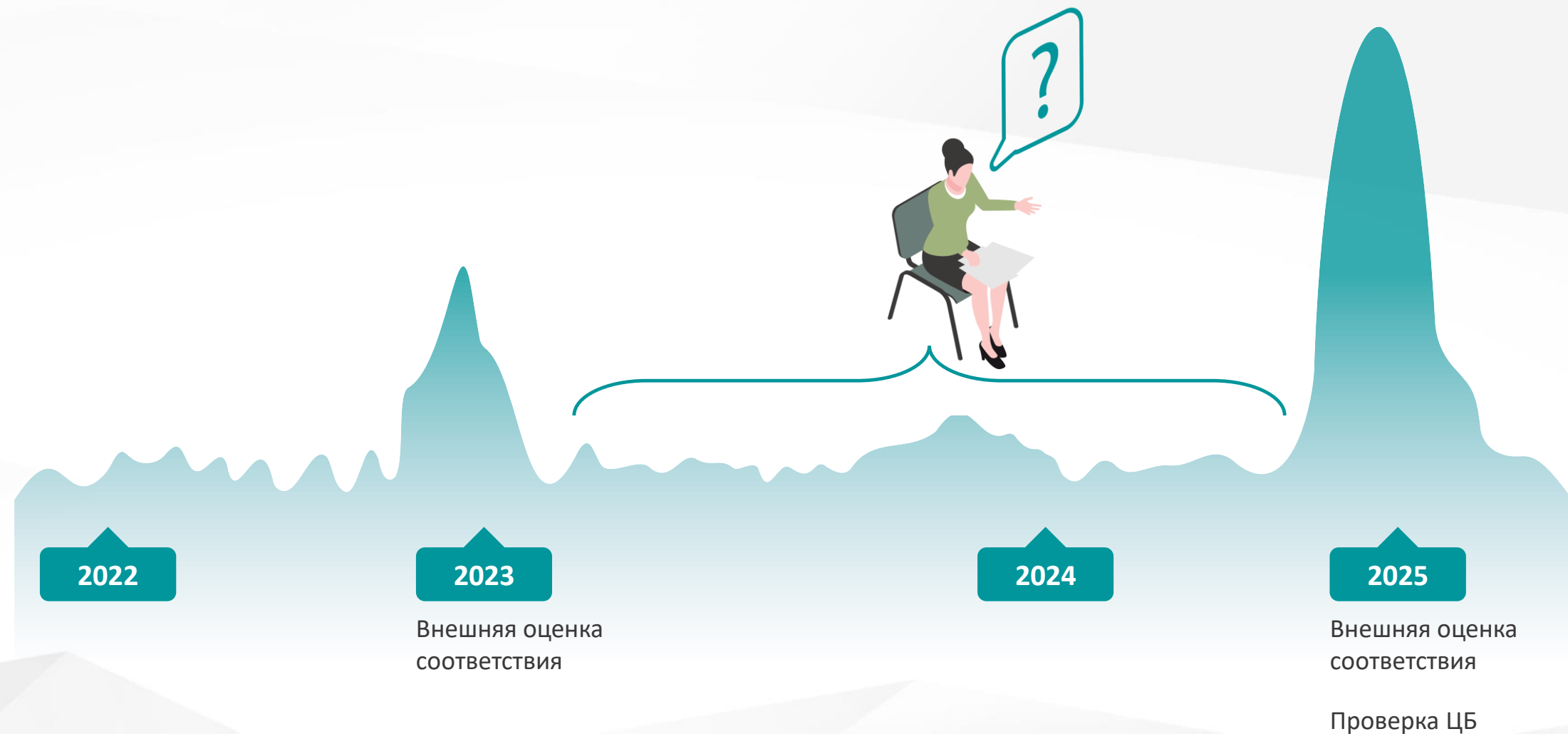
CISO

А пентест когда  
начинаем?

Мы придумали, как  
изменить бизнес-  
процессы

Подрядчик

# Уровень защищенности



# Как измерить уровень защищенности?

Внутренние проверки

Внешний аудит

OSINT

ASV-сканирование

Тест на проникновение

Red Team

Bug bounty

....

SOC

ГОСТ 57580



**ОТКАЗАНО**

**СОГЛАСОВАНО**

**Я ЭТОГО  
НЕ ВИДЕЛ**





Товарищ, у Вас УЗП упало!



# УЗП.1-УЗП.4, УЗП.13-16: Входят только те, кто реально работает



## Как проверить

- «Ручная» сверка
- Сканирование
- Правила в SIEM
- IDM
- RPA



## Вход

- **Данные из кадровой системы:** приказы о приеме, переводе, увольнении (ФИО работника, табельный номер, дата события)
- **Данные из AD** (активные учетные записи, дата последнего входа в систему)
- **Журналы событий** с контроллера домена, локальных АРМов, приложений: попытки входа, создание/включение УЗ
- **Реестр:** УЗ – табельный номер



## Выход

- Если все ОК – запись в журнал.
- Если не ОК:
  - **Отправить уведомление** в СИБ/админу,
  - **Зарегистрировать тикет** в системе учета инцидентов,
  - **Отключить УЗ,**
  - **Выгрузить** в тикет журналы событий, связанные с активацией УЗ, попытками входа, отключением/удалением УЗ,
  - Понизить оценку на **виджете.**



# УЗП.6-УЗП.12, УЗП.17-УЗП.21: Права есть только у тех, кому согласовано



## Как проверить

- «Ручная» сверка
- Сканирование
- Правила в SIEM
- IDM
- RPA



## Вход

- **Реестр:** ресурс\* – бизнес-владелец – матрица доступа
- **Результаты сканирования:** перечень выявленных ресурсов
- Журналы событий с контроллера домена, web-серверов, файловых серверов, локальных АРМов, почтового сервера, среды виртуализации, СУБД, сетевого оборудования, DHCP, DNS, DLP: создание/включение/отключение/ копирование ресурса, присвоение адреса, изменение прав, включение в группу



## Выход

- Если все ОК – запись в журнал.
- Если не ОК:
  - **Отправить уведомление** в СИБ/бизнес-владельцу,
  - **Зарегистрировать тикет** в системе учета инцидентов,
  - **Отключить ресурс / изменить сетевые правила / отозвать права доступа,**
  - **Выгрузить** в тикет связанные журналы событий,
  - Понизить оценку на **виджете.**





# УЗП.22-УЗП.28: события, связанные с управлением УЗ и правами, регистрируются



## Как проверить

- «Ручная» сверка целостности и доступности источников, хранилищ
- Правила в SIEM
- Лог-коллектор и система мониторинга доступности
- RPA



## Вход

- **Реестр:** ресурс\* или объект\*\* – источники журналов событий – особенности доступности источников
- **Результаты сканирования:** перечень выявленных ресурсов
- Журналы событий с контроллера домена, web-серверов, файловых серверов, локальных АРМов, почтового сервера, среды виртуализации, СУБД, сетевого оборудования, DHCP, DNS, DLP: создание/включение/отключение/копирование ресурса, присвоение адреса, изменение прав, включение в группу



## Выход

- Если все ОК – запись в журнал.
- Если не ОК:
  - **Отправить уведомление** в СИБ/админу,
  - **Зарегистрировать тикет** в системе учета инцидентов,
  - Понизить оценку на **виджете**.



# УЗП.29: Каждому АРМу и серверу по ответственному



## Как проверить

- «Ручная» проверка
- CMDB
- Сканирование
- Правила в SIEM
- RPA



## Вход

- **Реестр:** объект – ответственный
- **Данные бухучета**
- **Результаты сканирования:** перечень выявленных объектов
- **Журналы событий** с контроллера домена, антивируса, сетевого оборудования, DHCP, DNS, DLP: регистрация в сети, присвоение адреса, доменного имени, заведение в домен, включение в доменную группу



## Выход

- Если все ОК – запись в журнал.
- Если не ОК:
  - **Отправить уведомление** в СИБ/админу,
  - **Зарегистрировать тикет** в системе учета инцидентов,
  - **Изменить сетевые правила / отозвать права доступа,**
  - Выгрузить в тикет связанные **журналы событий,**
  - Понизить оценку **на виджете.**



# Что осталось?

УЗП.5

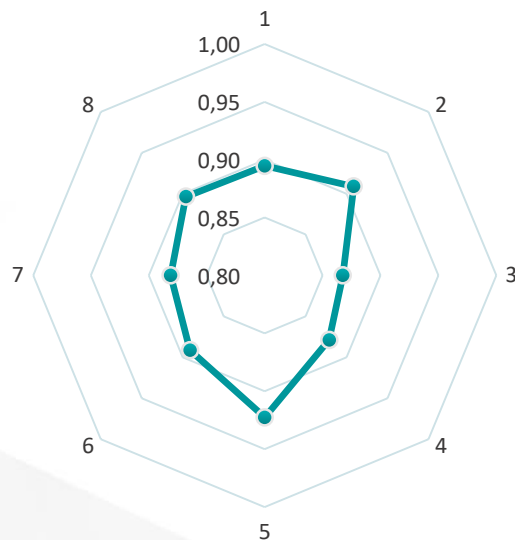
Документарное определение правил  
предоставления (отзыва) и блокирования  
логического доступа

Н

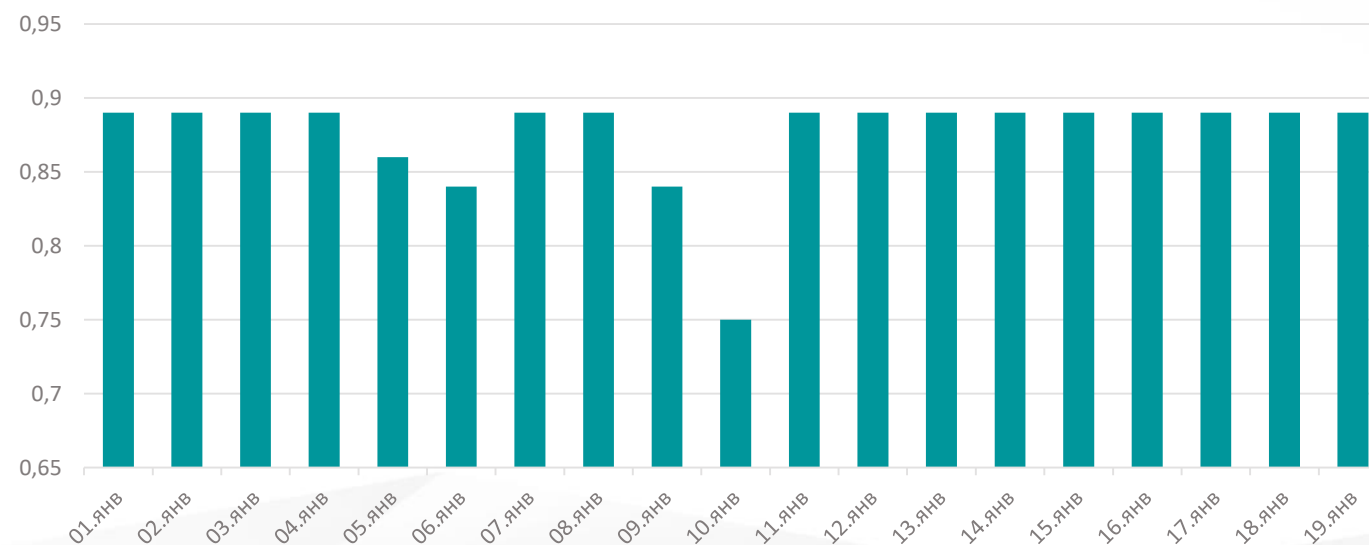
О

О

Итоговые оценки



УЗП



# Что не получится автоматизировать/роботизировать?

Ведение  
реестров



Закрытие  
инцидентов




Возврат оценки  
в исходное  
состояние







# Преимущества




Прозрачная  
методика




Понятные всем  
метрики




Можно посмотреть  
состояние «здесь и  
сейчас»



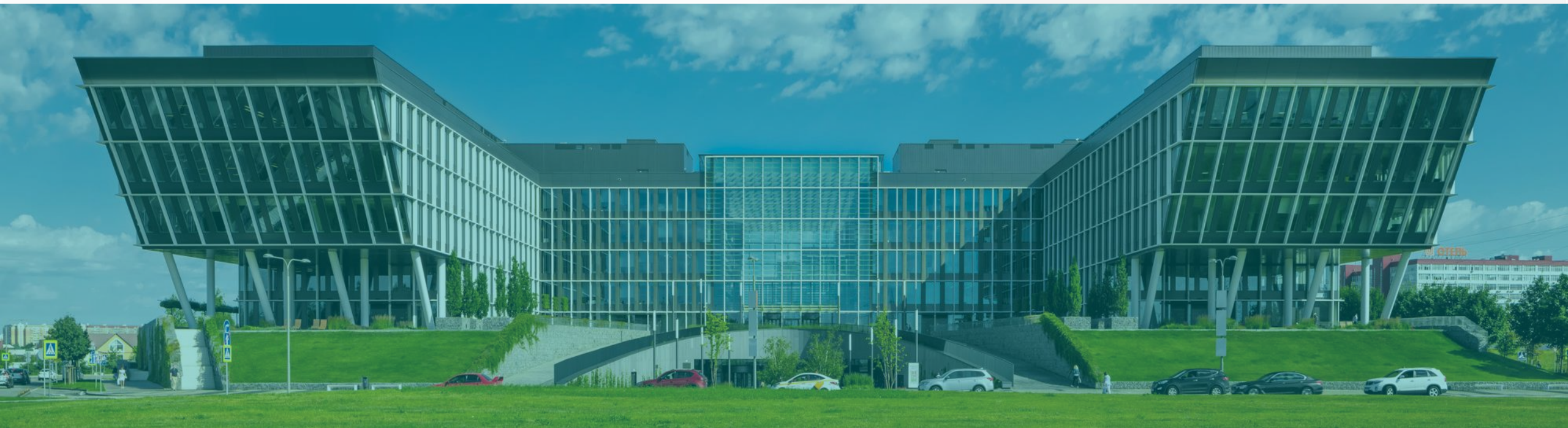
Легко  
отслеживать  
ретроспективу



Простота  
внедрения и  
сопровождения



Наглядные  
свидетельства  
при проверке



Россия, 108811, Москва, п. Московский,  
Киевское ш., 22-й км., вл. 6, стр.1, БП Comcity  
+ 7(495) 775 31 20, 363 01 33  
[info@step.ru](mailto:info@step.ru) | [step.ru](http://step.ru)