Научно-производственное республиканское
унитарное предприятие

НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Управление уязвимостями: новый взгляд на старую проблему

Борботько Тимофей Валентинович
д.т.н., профессор,
директор Государственного предприятия «НИИ ТЗИ»

Уязвимость

Уязвимость

недостаток **(слабость) программного (программно-технического)** ***средства или информационной системы в целом*****, который (которая) может быть использована для реализации угроз безопасности информации**

Объекты характеризующиеся такими недостатками

1. **Программное обеспечение**
2. **Корректность настройки программных и программно-технических средств**

Процесс управления уязвимостями

Актуальный **перечень активов** ***разделенных на группы*** **по уровню значимости**

Оценка наличия ***взаимосвязанных уязвимостей*** **для значимых активов**

Оценка степени критичности взаимосвязанных уязвимостей

Уязвимость 1

Приводит к локальному повышению привилегий и не требует взаимодействия с пользователем

Уязвимость 2

Позволяет внешнему нарушителю без аутентификации модифицировать файлы. Для успешной ее эксплуатации необходимо пользователю выполнить какое-либо действие, например перейти по ссылке

Уязвимость	Вектор CVSSv3	Оценка CVSSv3
Уязвимость 1	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	8.4
Уязвимость 2	AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N	4.3

Цепочка уязвимостей	Вектор CVSSv3	Оценка CVSSv3
Уязвимость 2 —> Уязвимость 1	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	8.8

CVSS COMMON VULNERABILITY SCORING SYSTEM

Оценка уязвимостей CVSS 3.0. https://habr.com/ru/companies/pt/articles/266485/

Процесс управления уязвимостями

Актуальный **перечень активов** ***разделенных на группы*** **по уровню значимости**

Оценка наличия ***взаимосвязанных уязвимостей*** **для значимых активов**

Перед устранением уязвимостей необходимо выполнить ***резервное копирование*** **(ПО, конфигурационные файлы и т.д.)**

Отсутствие уязвимости усложняет кибератаку для нарушителя

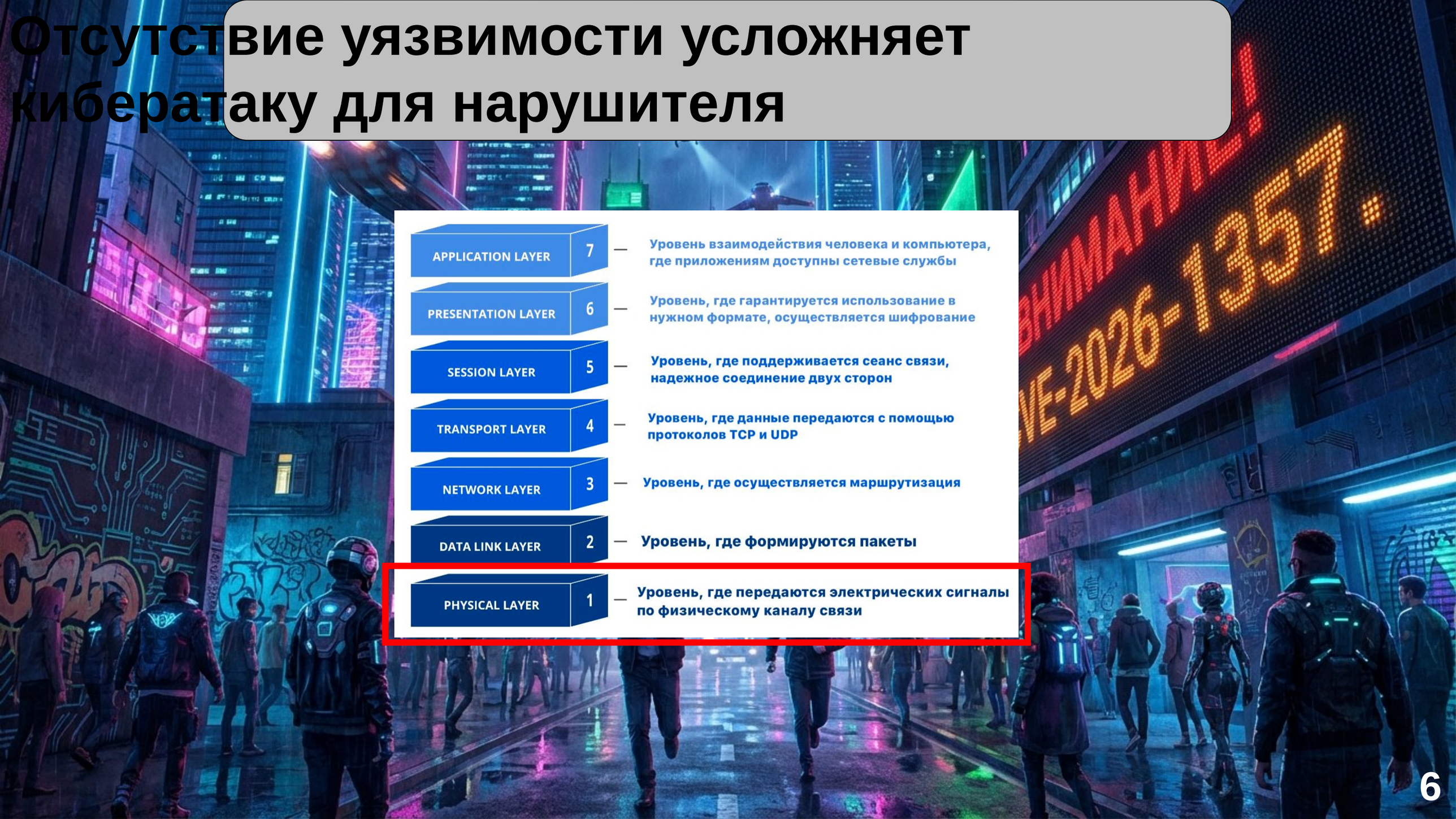
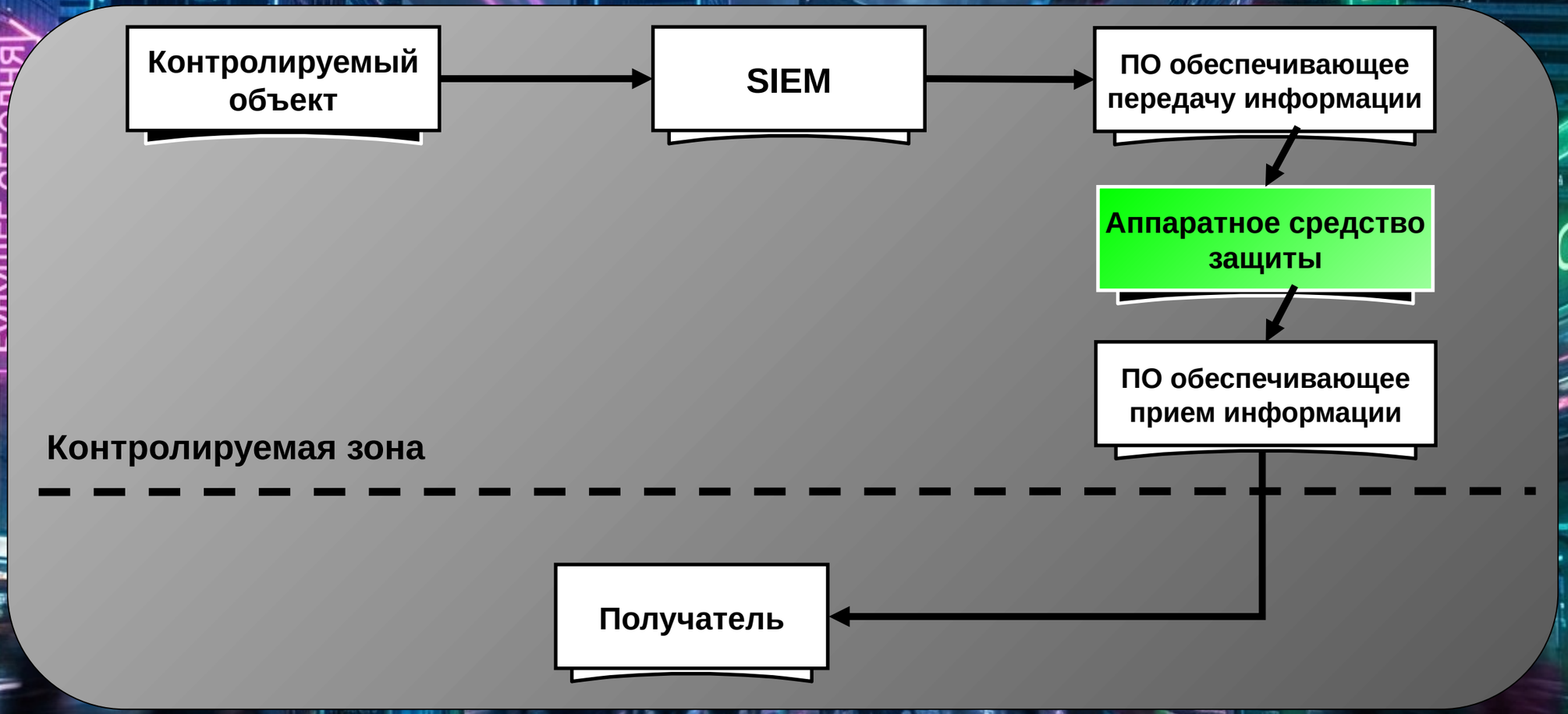


Схема включения аппаратного средства защиты



Научно-производственное республиканское
унитарное предприятие

НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Благодарю за внимание

Борботько Тимофей Валентинович
д.т.н., профессор,
директор Государственного предприятия «НИИ ТЗИ»