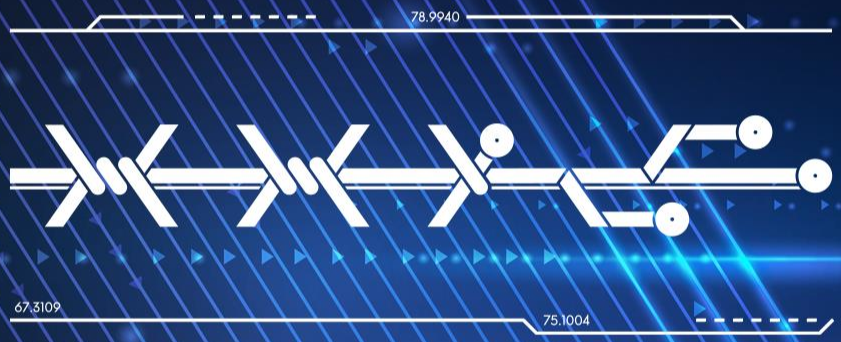
INFOWATCH®

ARMA ARMA



Применение СЗИ на внешней границе АСУТП

Игорь Душа
Директор по развитию продуктов,
Защита АСУТП, InfoWatch

2020

INFOWATCH®

Системы защиты на границе

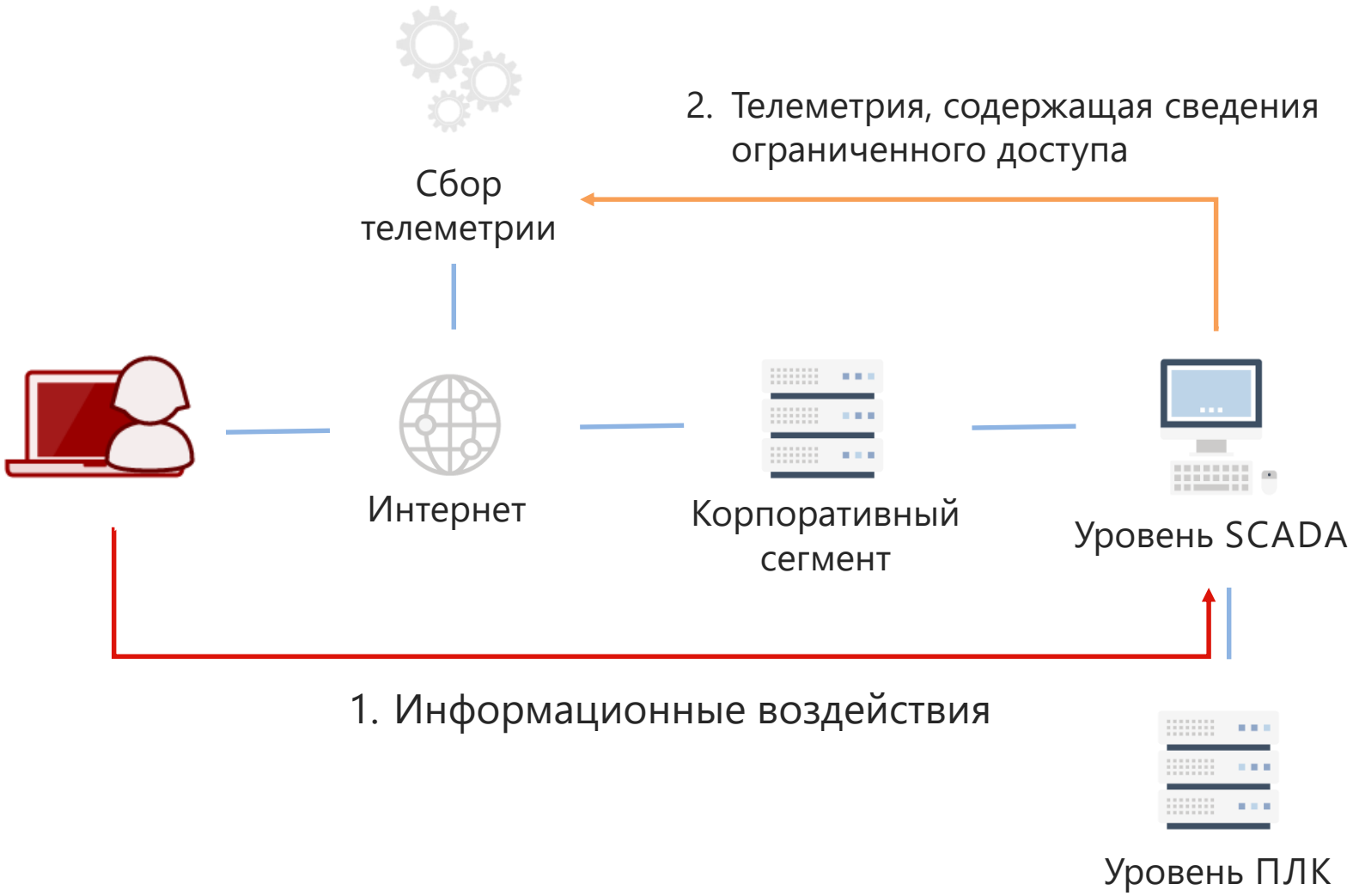
- Межсетевые экраны
- СОВ/СПВ
- Криптографические системы защиты
- Однонаправленные шлюзы
- Другие средства

INFOWATCH®

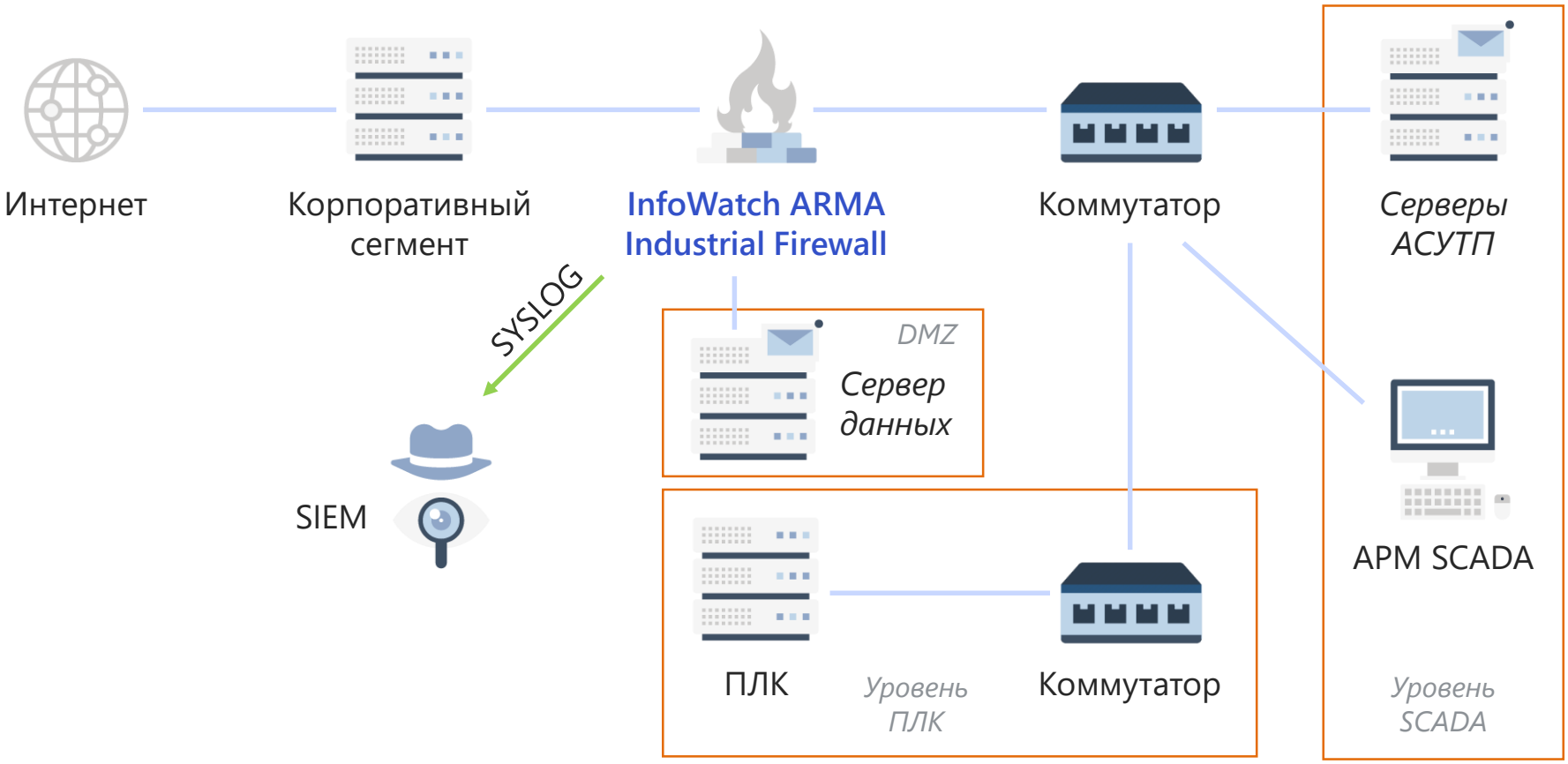
Варианты внешних подключений

- Соединение с корпоративным сегментом
- Техническая поддержка
- Смежные АСУ того же субъекта
- Соединение с кооперирующими предприятиями

Связь через корпоративный сегмент. Угрозы



Корпоративный сегмент. Защита



Связь через корпоративный сегмент. Итоги

INFOWATCH®

Защита соединения с корпоративным сегментом*

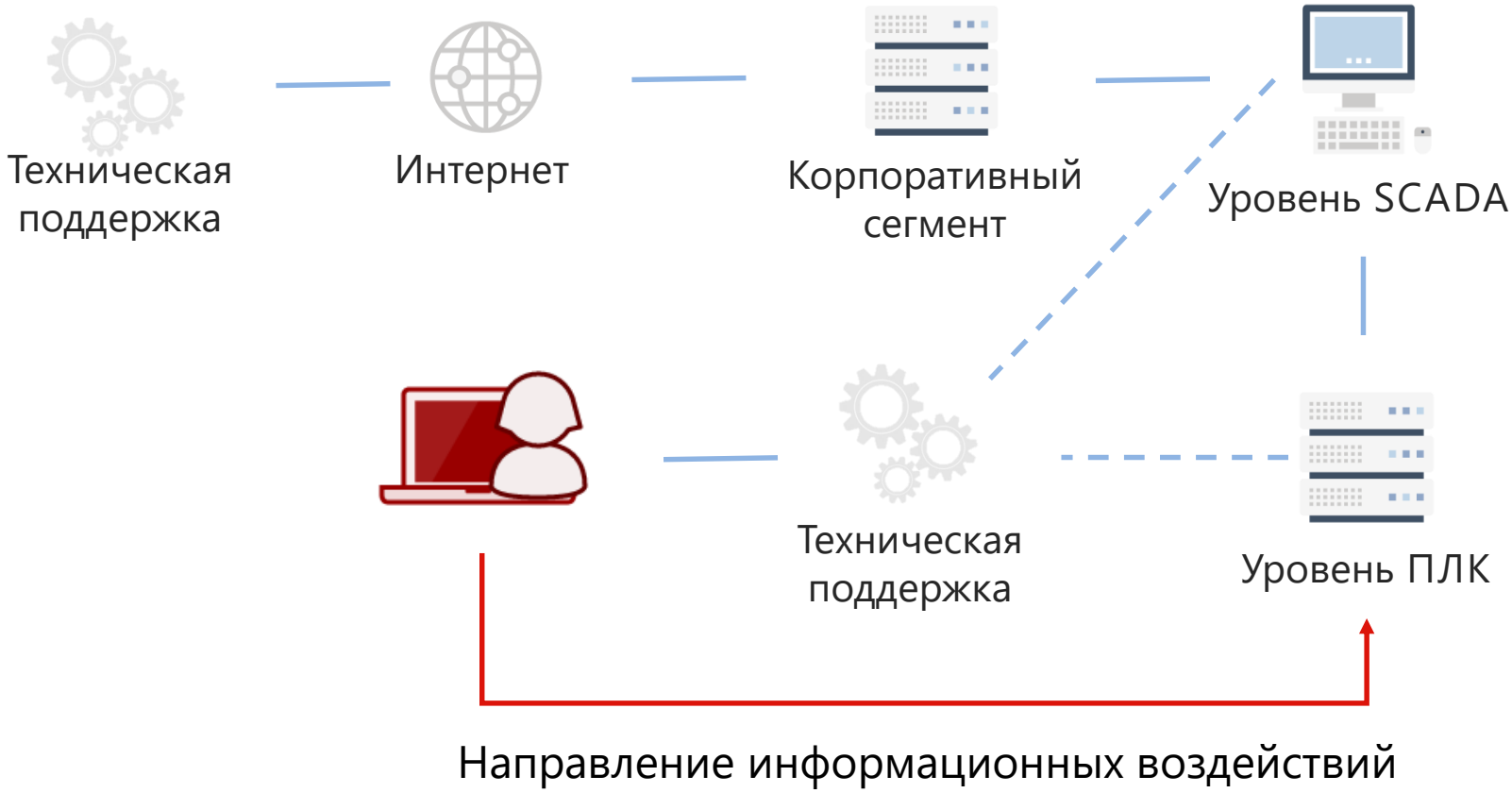
- При наличии соединения корпоративного сегмента и сегмента АСУ ТП необходимо разделение межсетевым экраном или однонаправленным шлюзом
- Протоколы должны быть четко регламентированы и отражены в политике, разрешаются только учтенные потоки
- Должен быть учтен риск раскрытия информации ограниченного доступа
- При необходимости может быть выделен DMZ

  Например, для выделения сервера исторических данных
- Желательно использование МЭ с функцией обнаружения/предотвращения вторжений

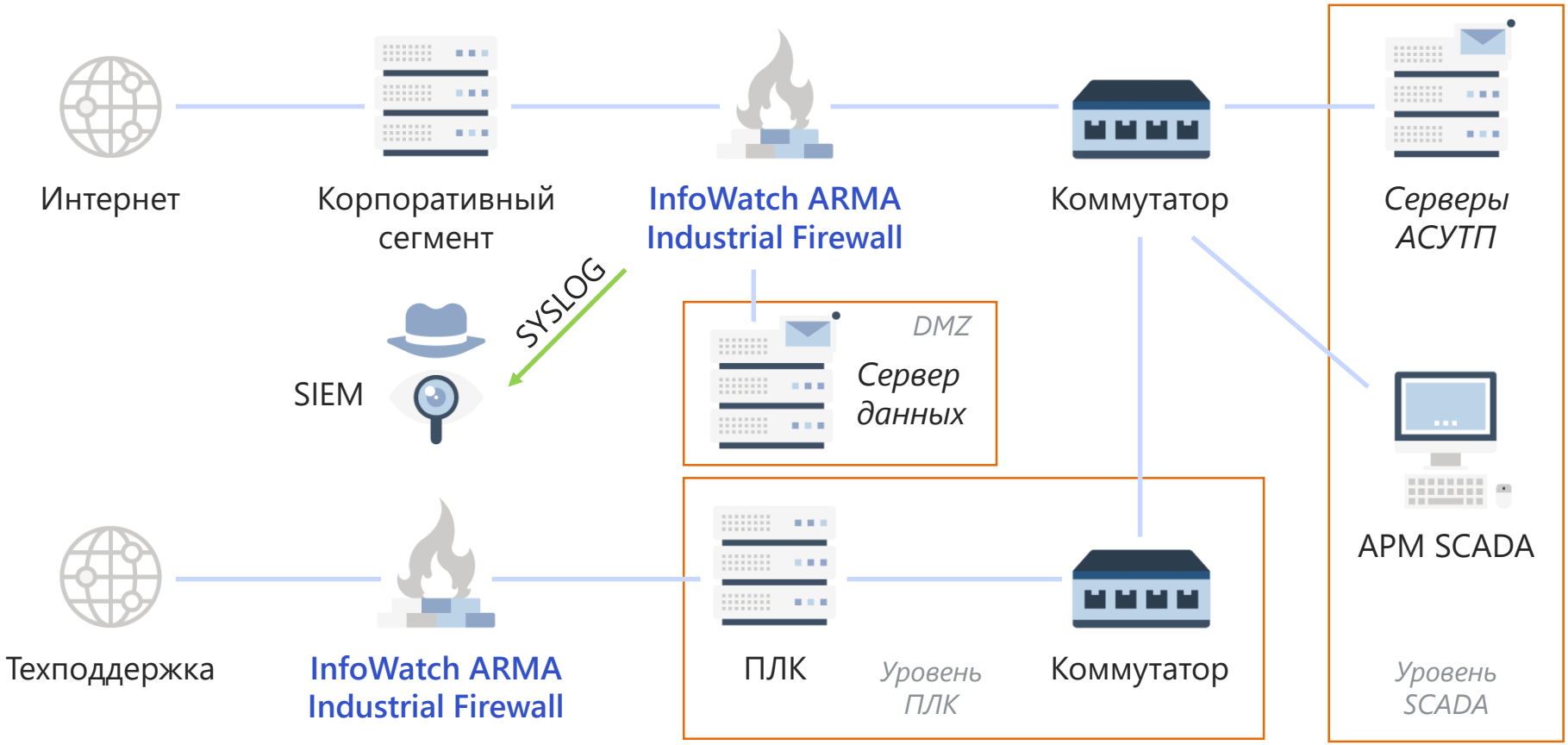
---

* Указаны лишь некоторые меры, полный список рекомендаций можно запросить на Igor.Dusha@infowatch.com

Техническая поддержка. Угрозы



Техническая поддержка. Защита



Техническая поддержка. Итоги

- Регламентация политики удаленного подключения
- Журналирование и мониторинг

  Должны записываться все действия. Крайне желателен разбор промышленного протокола для восприятия передаваемых данных
- Использование защищенного удаленного подключения
- Авторизация пользователей (например, на МЭ с помощью портала авторизации)

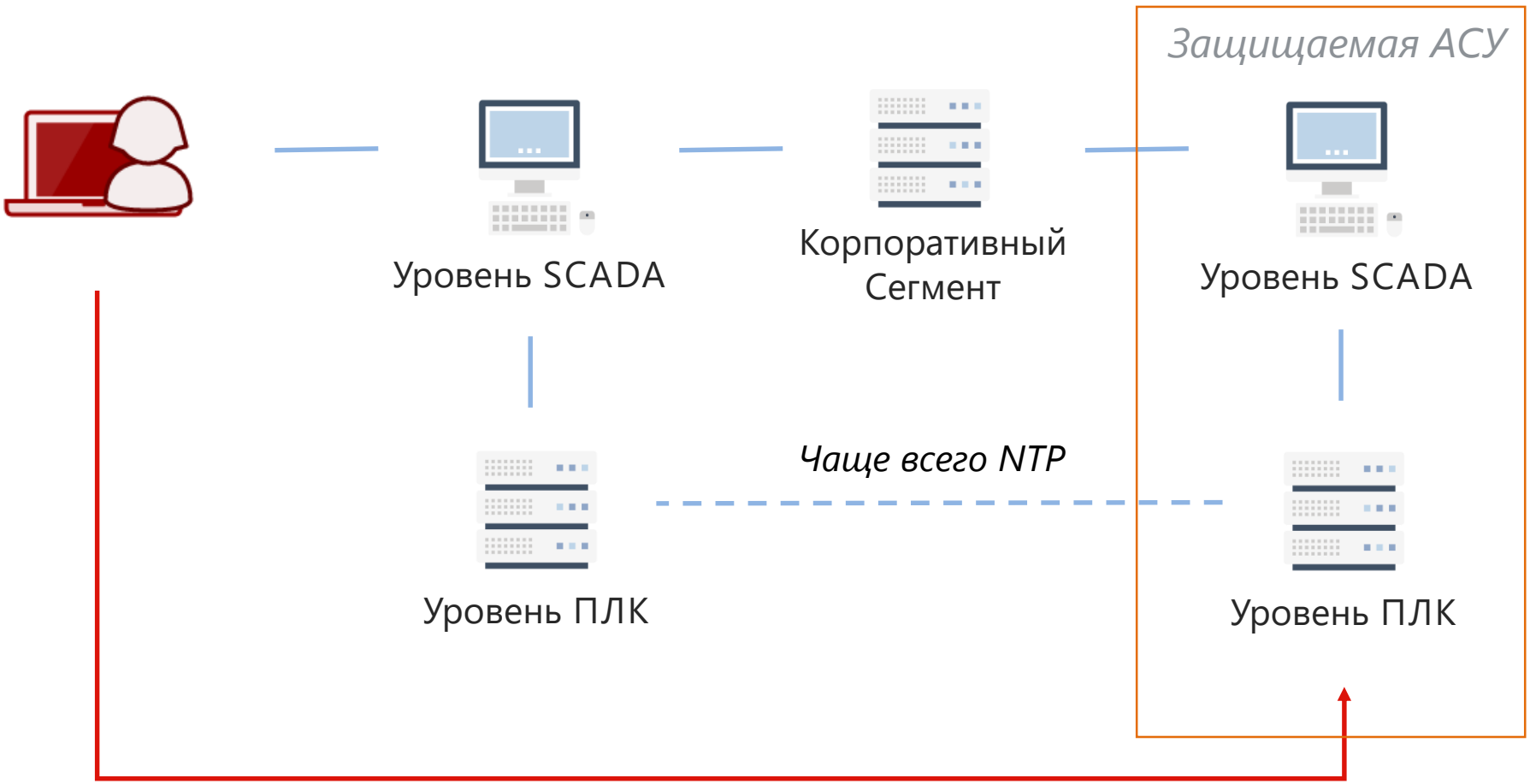
  Разграничение доступа пользователей (разных инженеров) к различным сетям
- Ограничение доступных действий

  Например, по умолчанию, доступно только чтение. Возможность изменения выдается по необходимости

---

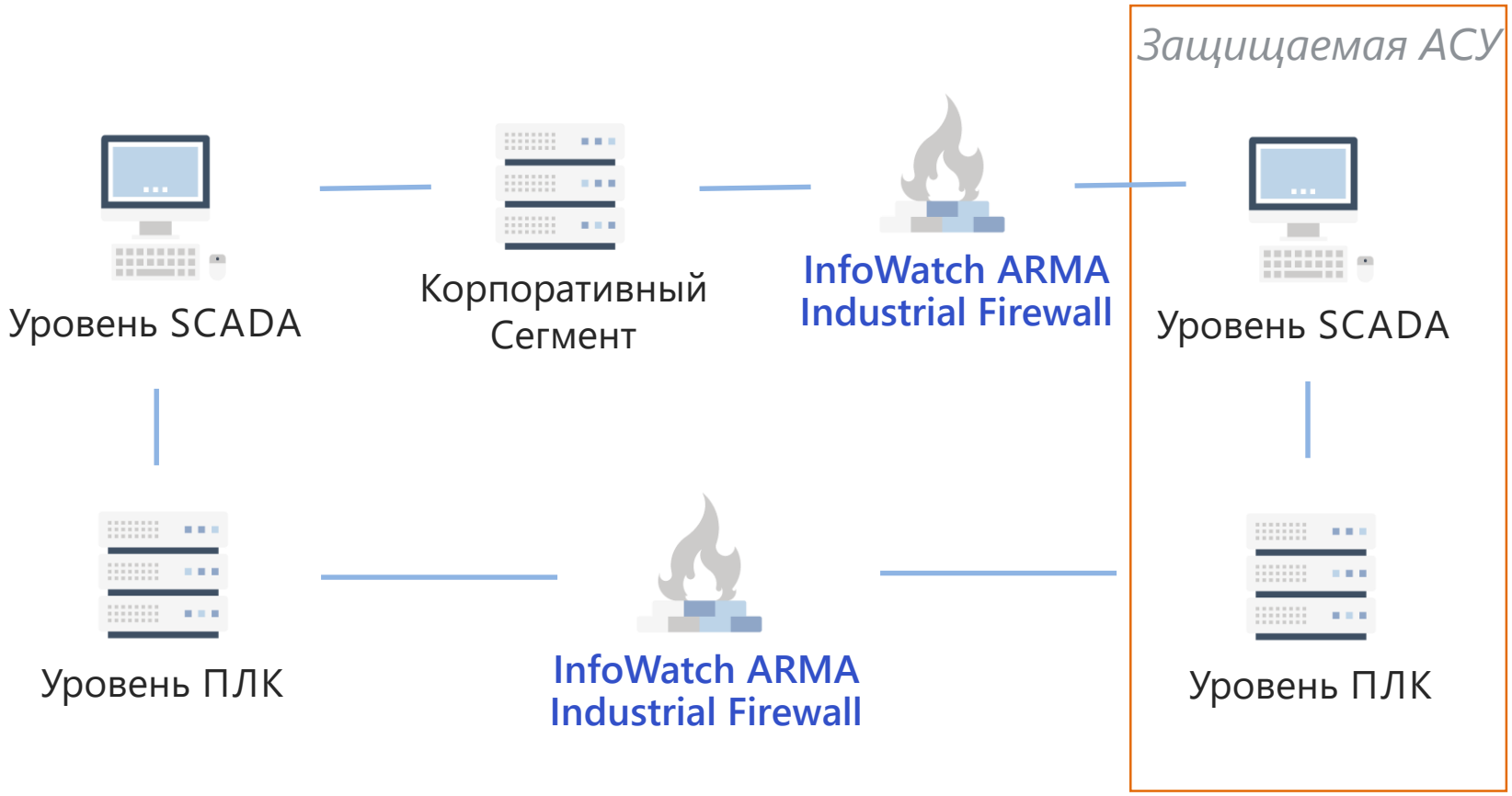
* Указаны лишь некоторые меры, полный список рекомендаций можно запросить на Igor.Dusha@infowatch.com

Смежные АСУ. Угрозы



Направление информационных воздействий

Смежные АСУ. Защита



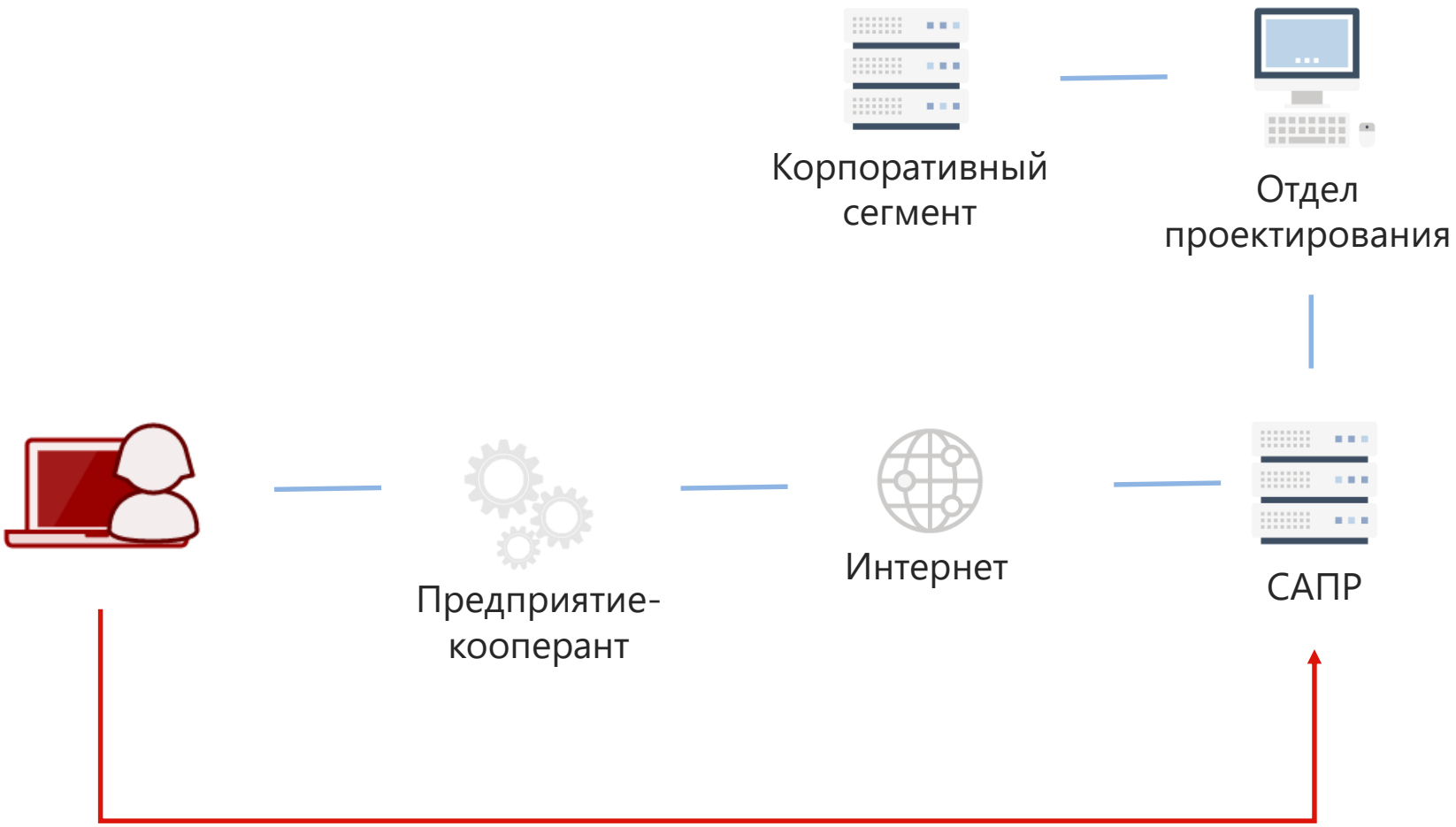
Смежные АСУ. Итоги

- Если смежные АСУ — это системы разного уровня безопасности, то должны быть разделены средствами защиты информации
- Обязательно должны быть регламентированы и определены информационные потоки
- Определенные в политике потоки должны быть ограничены на МЭ
- Может использоваться плоская сеть, для нее возможна настройка в прозрачном режиме (на L2)

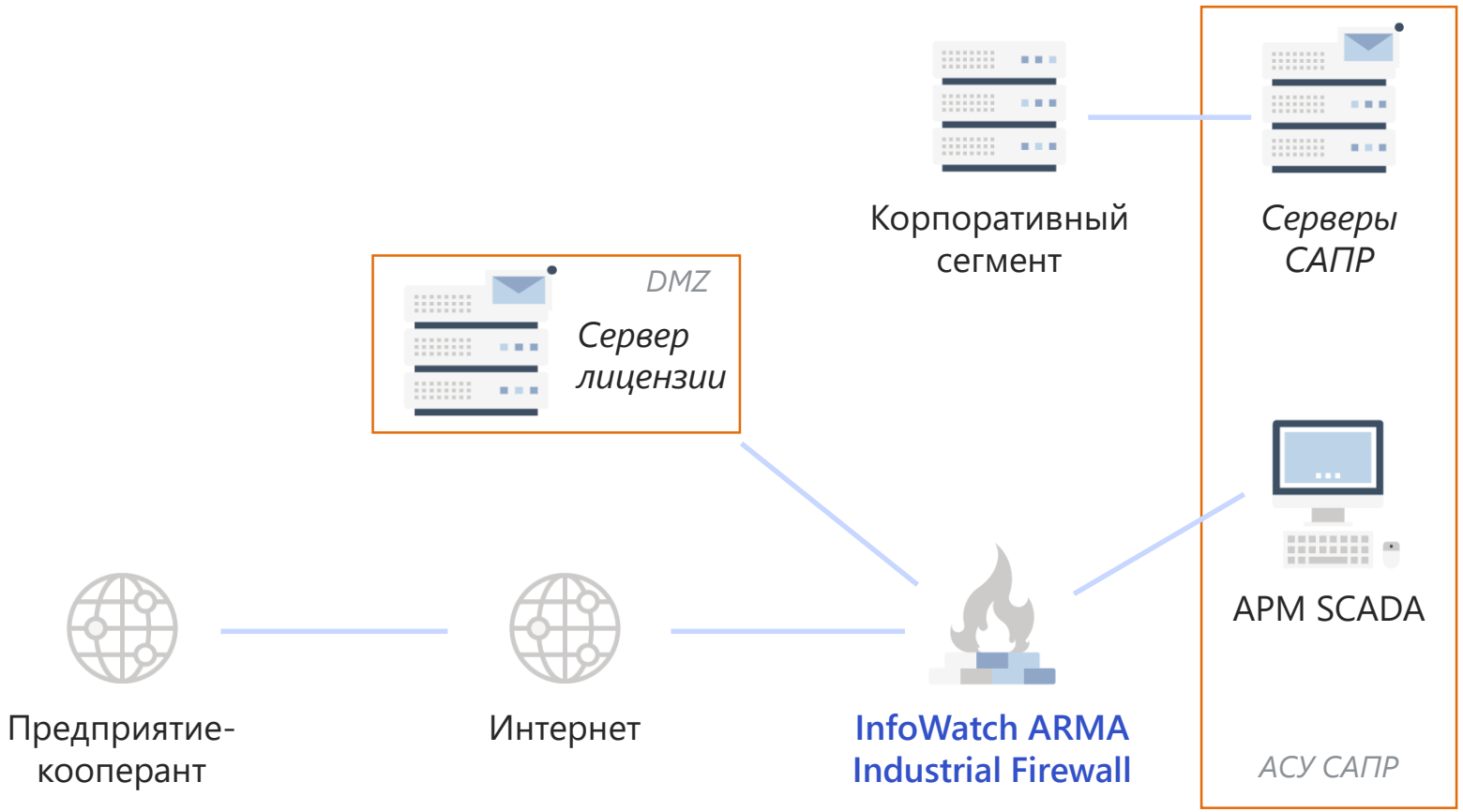
---

* Указаны лишь некоторые меры, полный список рекомендаций можно запросить на Igor.Dusha@infowatch.com

Кооперант. Угрозы



Кооперант. Защита



Кооперант. Итоги

- Обязательное наличие защищенного соединения
- Регламентация политики удаленного подключения
- Ограничение доступных действий и используемых информационных потоков
- Разрешаются информационные потоки только между определенными заранее машинами/пользователями и для определенных информационных потоков

---

* Указаны лишь некоторые меры, полный список рекомендаций можно запросить на Igor.Dusha@infowatch.com

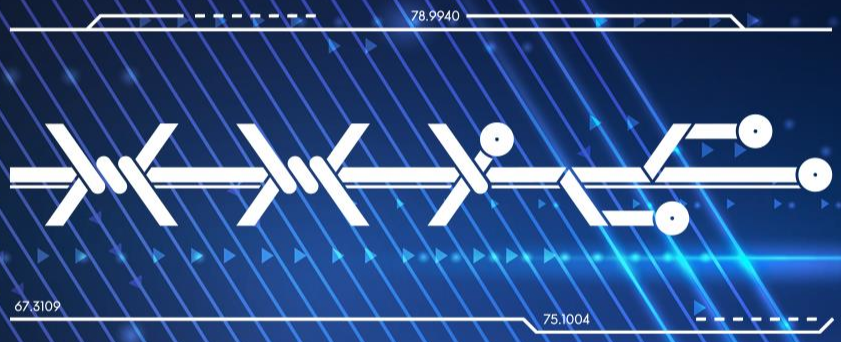
INFOWATCH®

Заключение

- Все внешние подключения к АСУ должны контролироваться
- МЭ — это не только средство ограничения подключения, но и средство журналирования и средство мониторинга
- Необходимо руководствоваться принципом наименьших привилегий

INFOWATCH®

ARMA ARMA



СЗИ для АСУТП ждет вас на стенде InfoWatch

/InfoWatchOut

/InfoWatch

infowatch.ru

INFOWATCH®

ARMA ARMA

Пряники ждут там же!!

/InfoWatchOut

/InfoWatch

infowatch.ru