kaspersky

Kaspersky Industrial Cybersecurity Conference 2020

Ян Сухих

Менеджер по развитию бизнеса Кибербезопасности АСУ ТП, Руководитель отдела, Ростелеком-Солар

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

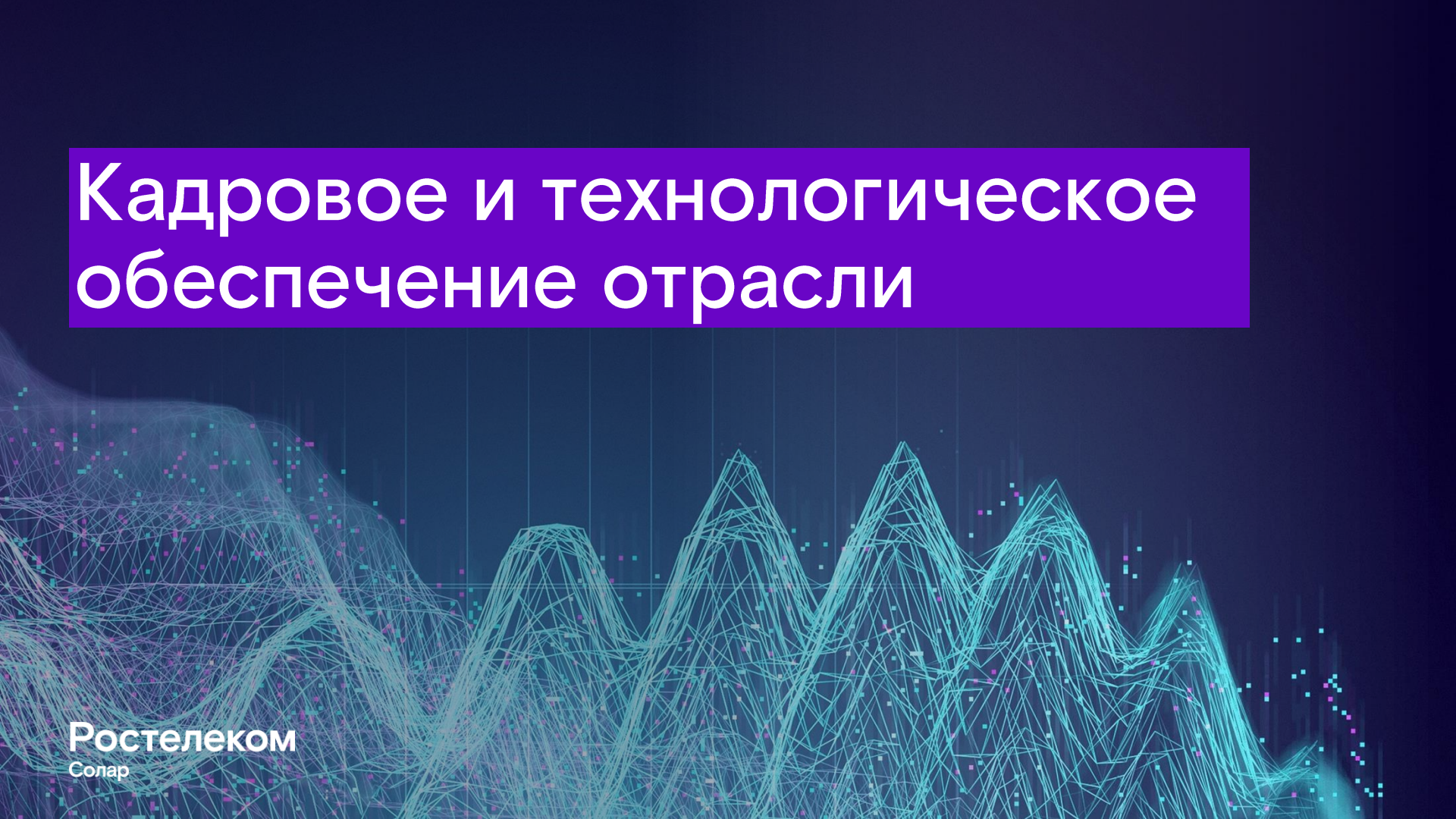
Аутсорсинг ИБ АСУ ТП

Миф или реальность?

Сухих Ян Андреевич
y.sukhikh@rt-solar.ru

Ростелеком
Солар

Кадровое и технологическое обеспечение отрасли



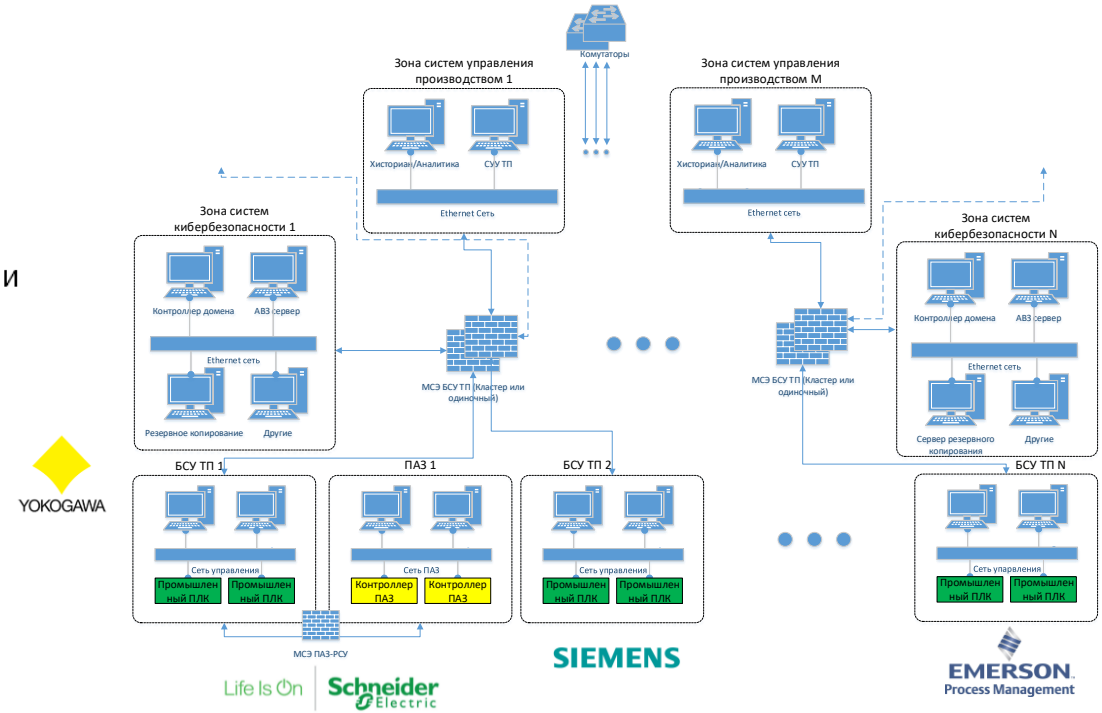
Ростелеком
Солар

Зоопарк вендоров (АСУ ТП и СрЗИ)

- АСУ ТП разных вендоров и разных поколений
- Зоопарк сетевого оборудования и сетевых архитектур
- Ситуация усугубляется, когда защиту АСУ ТП выполняют разные организации без соблюдения единых технических политик. Создается зоопарк средств и способов защиты информации + зоопарк ОРД

Лекарство:

- Разработка единой концепции
- Строгий контроль за решениями вендоров АСУ ТП/интеграторов



https://bit.mephi.ru/index.php/bit/article/download/1274/1191

Кадровое обеспечение

- Тотальный дефицит кадров на рынке, который будет только усугубляться
- Дефицит усугубляется низким уровнем автоматизации СЗИ и имеющимся зоопарком
- Высокие денежные и временные затраты на наем и обучение, обученный человек уходит в СИ или вендора или уезжает за границу
- Подготовленные кадры с большой вероятностью перейдут в интеграторов или вендоров

Лекарство:

- Аутсорсинг
- Взвешенный продуманный подход к построению СЗИ
- Сотрудничество с профильными вузами

Ростелеком
Солар

Цена ошибки

Ущерб от останова производства на химическом предприятия обычно составляет от 0,5 млн $ до 3 млн $ в сутки

Время простоя при внезапном останове может составлять от нескольких часов до нескольких суток

Потенциальный ущерб от крупных аварий может исчисляться десятками миллиардов $

Ущерб от крупнейшей в истории BP техногенной катастрофы на январь 2018 составил около 65 млрд $

https://goo-gl.su/IdbKKjB

Потери Maersk от кибератаки оцениваются в 300 млн $

https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff

Возможные пути?

1. **Все сами!**
   Создание полноценной СЗИ от АВЗ до SIEM/SGRC/IRP/SOAR

- Независимость и ощущение полного контроля (+)
- Дорого (-)
- Может не хватать компетенций, соответственно качество СЗИ будет недостаточным (-)

2. **Все на аутсорсинг! Фокусируемся на основной деятельности**
   Вся кибербезопасность как сервис

- Зависимость от поставщиков сервисных услуг (-)
- Прогнозируемые затраты, легко масштабировать (+)
- Нет своего персонала по ИБ (+/-)

3. **Гибридная модель**
   Основные базовые системы свои, обслуживаются собственным персоналом. Высокоуровневые сложные и дорогие системы на аутсорсинг

- Ключевые компетенции свои (+)
- Контроль за ключевыми процессами (+)
- Экономия (+)
- Частичная зависимость от сервисной организации (-)

Про наш опыт и предложение расскажет...

Сиянов Виталий Антонович

v.siyanov@rt-solar.ru

- Менеджер по развитию направления кибербезопасности АСУ ТП Solution Sale
- Автор публикаций и исследований по защите АСУ ТП и КИИ
- Участник сообщества RUSCADASEC

Наш опыт

Ростелеком
Солар

Гибридная модель аутсорсинга

С JSOC

Только самое необходимое

Но под надежным присмотром

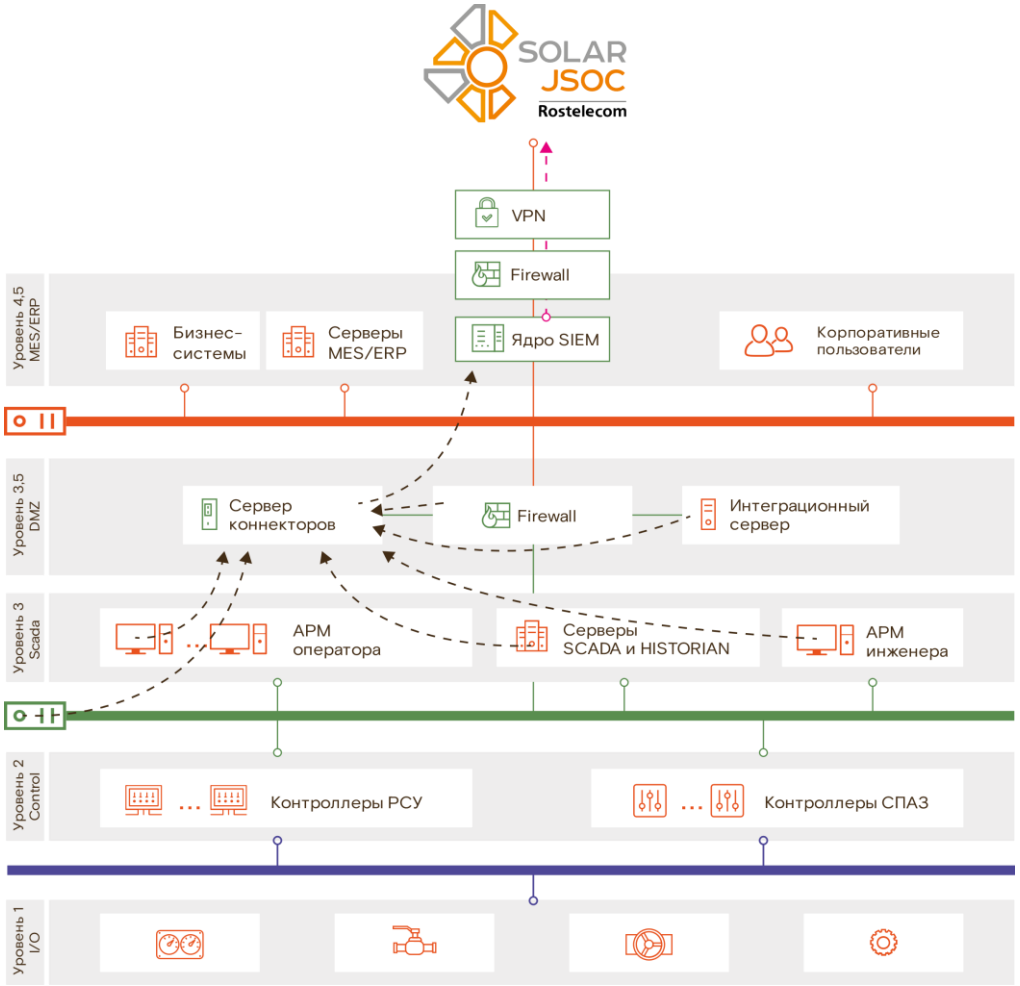
Без JSOC

Максимальная защита, нежизнеспособен без поддержки

Ростелеком
Солар

Гибридное подключение

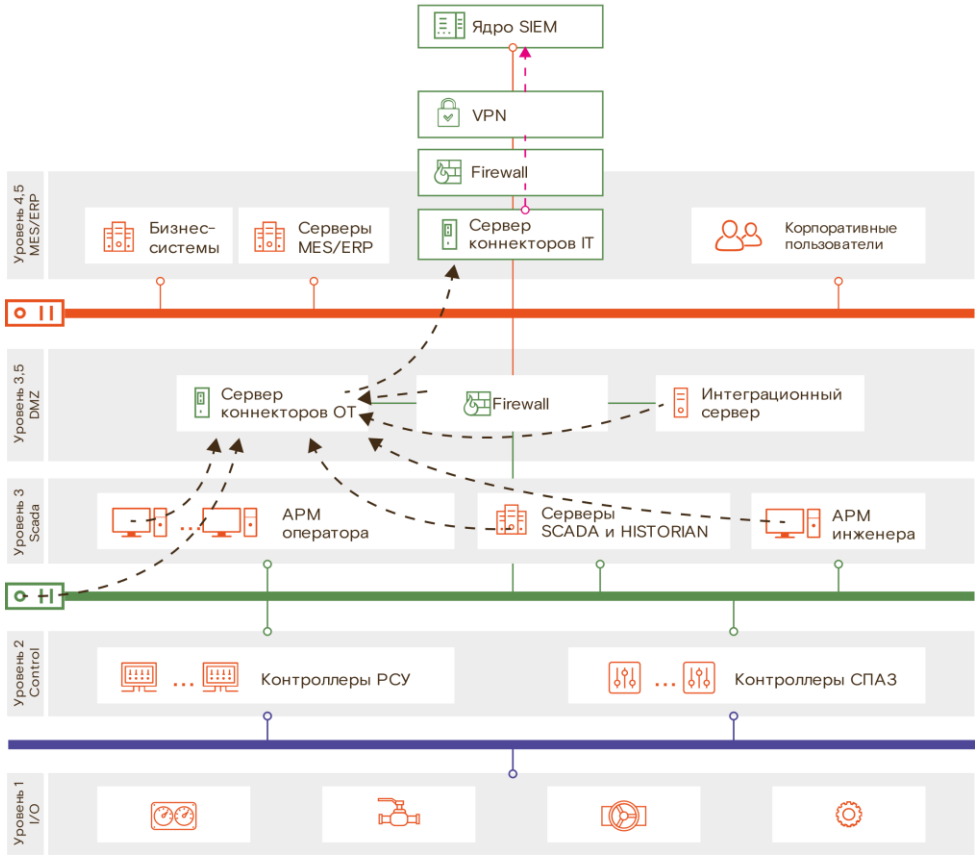
- В инфраструктуре заказчика развернута и настроена собственная SIEM-система
- События информационной безопасности от АСУ ТП поступают и обрабатываются непосредственно в SIEM заказчика
- Специалисты Solar JSOC подключаются к SIEM заказчика по защищенному каналу связи (site-to-site VPN) и осуществляют процесс мониторинга и реагирования на события и инциденты



Ростелеком
Солар

Облачное подключение

- В корпоративной или технологической инфраструктуре заказчика отсутствует собственный SIEM.
- События от АСУ ТП собираются и обрабатываются в облачном SIEM в ЦОД Solar JSOC
- Передача событий из технологической инфраструктуры заказчика осуществляется по защищенному каналу связи (site-to-site VPN) с организацией процесса мониторинга и реагирования на события и инциденты



Ростелеком
Солар

Источники событий

Промышленное оборудование и ПО:

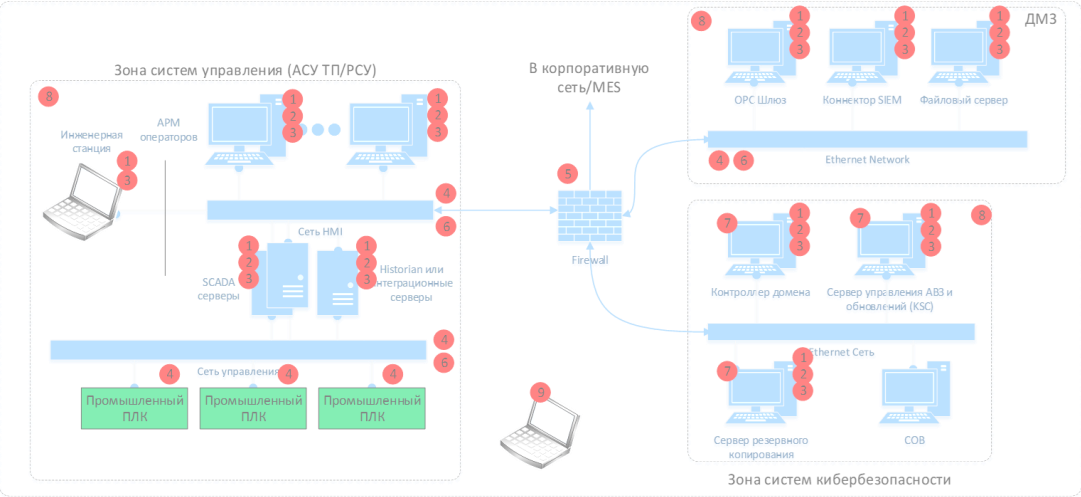
- Промышленные контроллеры (в которых есть возможность передачи событий)
- Промышленное сетевое оборудование
- Специализированное прикладное программное обеспечение (в работе)
- Промышленные СрЗИ

Традиционное оборудование и ПО:

- МСЭ
- Операционные системы
- Традиционные СрЗИ

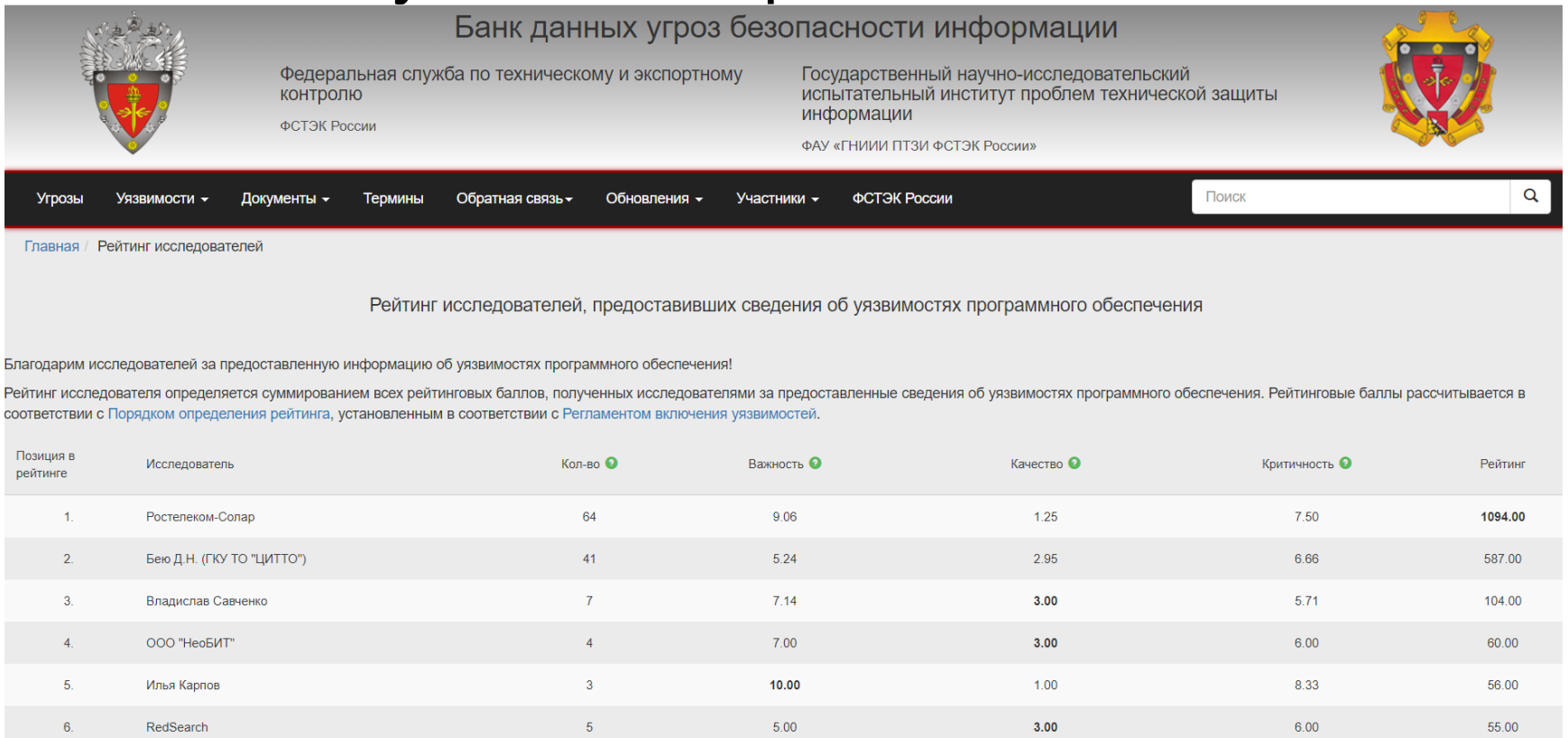
Разработка уникальных правил детектов:

- На основе результатов исследования
- защищенности



Ростелеком
Солар

Собственные уникальные правила детектов



Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю

ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической защиты информации

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Угрозы | Уязвимости | Документы | Термины | Обратная связь | Обновления | Участники | ФСТЭК России | Поиск

Главная / Рейтинг исследователей

Рейтинг исследователей, предоставивших сведения об уязвимостях программного обеспечения

Благодарим исследователей за предоставленную информацию об уязвимостях программного обеспечения!

Рейтинг исследователя определяется суммированием всех рейтинговых баллов, полученных исследователями за предоставленные сведения об уязвимостях программного обеспечения. Рейтинговые баллы рассчитываются в соответствии с Порядком определения рейтинга, установленным в соответствии с Регламентом включения уязвимостей.

Позиция в рейтинге	Исследователь	Кол-во	Важность	Качество	Критичность	Рейтинг
1.	Ростелеком-Солар	64	9.06	1.25	7.50	**1094.00**
2.	Бею Д.Н. (ГКУ ТО "ЦИТТО")	41	5.24	2.95	6.66	587.00
3.	Владислав Савченко	7	7.14	**3.00**	5.71	104.00
4.	ООО "НеоБИТ"	4	7.00	**3.00**	6.00	60.00
5.	Илья Карпов	3	**10.00**	1.00	8.33	56.00
6.	RedSearch	5	5.00	**3.00**	6.00	55.00

Ростелеком
Солар

Спасибо за внимание!

Остались вопросы?

Пишите на

y.sukhikh@rt-solar.ru
v.siyanov@rt-solar.ru

Ростелеком
Солар

Контакты

Центральный офис

125009 г. Москва,
Никитский переулок, 7с1

+7 (499) 755-07-70

info@rt-solar.ru

Ростелеком
Солар