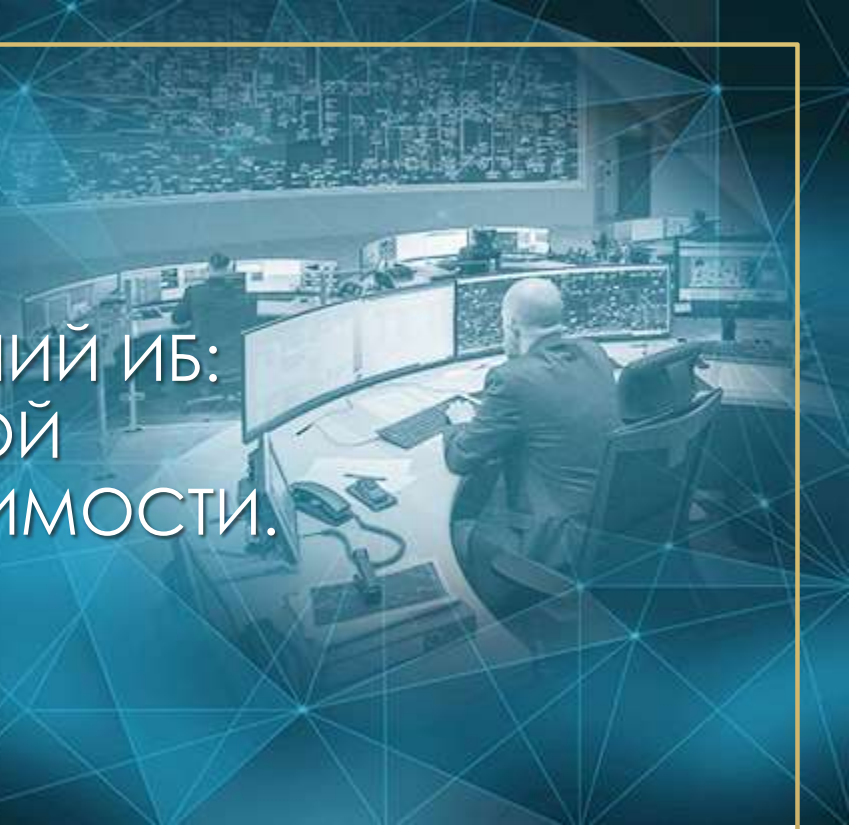
СИСТЕМНЫЙ ОПЕРАТОР
ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ
RUSSIAN POWER SYSTEM OPERATOR



# РЫНОК ОТЕЧЕСТВЕННЫХ РЕШЕНИЙ ИБ: ДВИЖЕНИЕ В СТОРОНУ ПОЛНОЙ ТЕХНОЛОГИЧЕСКОЙ НЕЗАВИСИМОСТИ. ОПЫТ ИМПОРТОЗАМЕЩЕНИЯ.

**Александр Капустин**
Заместитель начальника службы ИБ АО «СО ЕЭС»,
зам. руководителя ЭГ по кибербезопасности АЦЭ

# СИСТЕМНЫЙ ОПЕРАТОР ЕЭС



**Структура Общества**

ИА с центральным диспетчерским управлением

7 объединенных диспетчерских управлений

49 региональных диспетчерских управлений

11 представительств

**Основные задачи**

- Планирование и управление технологическими режимами работы объектов ЕЭС России в реальном времени
- Обеспечение перспективного развития ЕЭС России
- обеспечение единства и эффективной работы технологических механизмов оптового и розничных рынков электрической энергии и мощности

**ИТ и ИБ**
1840 человек

# ОСНОВНЫЕ ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА



| | |
|---|---|
| Указ Президента РФ от 30 марта 2022 г. № 166 | Запрещает использовать иностранное ПО на ЗОКИИ |
| Указ Президента РФ от 1 мая 2022 г. № 250 | Запрещает использовать средства защиты информации, странами происхождения которых являются недружественные иностранные государства |
| Требования к ПО, утвержденные постановление Правительства РФ от 22 августа 2022 г. № 1478 | Импортонезависимое ПО:<br>1) должно быть включено в реестр российских программ<br>2) ПО для обеспечения безопасности ЗОКИИ (для реагирования на КА и КИ) должно соответствовать требованиям, установленным ФСТЭК России и (или) ФСБ России, что должно быть подтверждено соответствующим документом (сертификатом) |
| Постановление Правительства РФ от 14.11.2023 № 1912 | Доверенный ПАК - ПАК, который соответствует одновременно трем критериям:<br>1) Сведения о ПАК содержатся в едином реестре российской радиоэлектронной продукции<br>2) В составе ПАК «импортонезависимое» ПО<br>3) ПАК, в случае реализации в нем функций защиты информации, соответствует требованиям, установленным ФСТЭК России и (или) ФСБ России, что должно быть подтверждено соответствующим документов (сертификатом) |

# ПРОЦЕСС ДВИЖЕНИЯ К ТЕХНОЛОГИЧЕСКОЙ НЕЗАВИСИМОСТИ В ИБ



**Шаг 1**
Инвентаризация

**Шаг 2**
Разработка плана (в т.ч. на базе отраслевого)

**Шаг 3**
Утверждение плана и отправка в регулирующие органы

**Шаг 4**
Реализация, но не позднее обозначенных в НПА сроков:
- для ПО до 01.01.2025;
- для ПАК до 01.01.2030.

## СТАТИСТИКА ПО ПРОТЕСТИРОВАННЫМ ОТЕЧЕСТВЕННЫМ РЕШЕНИЯМ

- С 2015 г. проведено тестирование более 80 российских решений
- 50% протестированного ПО и ПАК оказались не готовым к дальнейшему использованию
- 45% рекомендованы с учетом существенной доработки
- Лишь 5% введены в эксплуатацию с минимальными нареканиями
- Пик наиболее приближенных к успеху тестирований пришелся на 2021 - 2023 год

**Процедура одинакова для ПО и для ПАКов, но требуется синхронизация требований разных регуляторов**

# ОСНОВНЫЕ ПРОБЛЕМНЫЕ МОМЕНТЫ ПРИ ВНЕДРЕНИИ ОТЕЧЕСТВЕННЫХ РЕШЕНИЙ ИБ В ОТДЕЛЬНОЙ КОМПАНИИ



## ФАКТЫ

- Производители продают RoadMap, а не действительно реализованный функционал
- Большинство отечественных продуктов «сырые» как по качеству кода, так и в силу отсутствия документации
- Не выстроена тех поддержка, либо отсутствуют SLA, либо его не придерживаются
- Нет преемственности продуктовой линейки *(либо в рамках одной ветки версий надо обновляться с чистой установки, либо вендор «хоронит» продукт и за дополнительную плату предлагает перейти на новый продукт)*

## СЛЕДСТВИЯ

- Внедряются средства защиты и существенными нестыковками функционала
- Внедрение и сопровождение скорее похоже на НИР, а не осознанный процесс
- Проблематично встраивать в систему новые разрекламированные решения
- Нет смысла качественно внедрять продукт, так как новая версия все равно потребует все переделать

**Отдел ИБ приносит в работу компании одни проблемы и неудобства**

# ОСНОВНЫЕ ПРОБЛЕМНЫЕ ОБЛАСТИ ПРИ ВНЕДРЕНИИ ОТЕЧЕСТВЕННЫХ РЕШЕНИЙ ИБ В КРУПНОМ ПРЕДПРИЯТИИ



## ФАКТЫ

- Надежность
- Непрерывность
- Производительность
- Управляемость
- Наблюдаемость
- Предсказуемость развития

## СЛЕДСТВИЯ

- Трудности (порой непреодолимые) при проектировании и внедрении сложных решений
- Расходы и на внедрение, и на эксплуатацию отечественного продукта выше в 3 раза
- Очень многое приходится писать самостоятельно

**Службы ИБ и ИТ являются незримыми жертвами обстоятельств**

# ПРОБЛЕМЫ ОТЕЧЕСТВЕННЫХ РЕШЕНИЙ ИБ (ПРАКТИЧЕСКИЕ КЕЙСЫ)



| Тип решения | Выявленные проблемы |
|---|---|
| **PAM (Privileged Access Management)** | В решении используется уязвимый протокол TLS v1.1, с 2020 года разработчик не может внедрить TLS v1.2 и выше. *(протокол TLS v1.2 существует с 2008 года, TLS 1.3 в марте 2018 года)* |
| **WAF (Web Application Firewall)** | В конце 2018 года ПО было внедрено и в процессе постепенного перевода под защиту WAF был зафиксирован ряд замечаний:<br>• нестабильная работа механизма отказоустойчивости<br>• отсутствие механизма аутентификации пользователей по сертификатам<br>• проблема с распознаванием атак типа «Bruteforce»<br>Указанные проблемы разработчиком исправлены не были. **В 2021 году разработчик прекратил развитие, поддержку и продажу продукта.** |
| **ACS (Access Control Server) AAA (Authentication, Authorization, Acconting) 802.1x** | В процессе эксплуатации с 2021 года были выявлены критические замечания:<br>• некорректная работа протокола TACACS<br>• отсутствие поддержки динамических списков доступа<br>**Разработчик отказался исправлять замечания и в начале 2023 года предложил приобрести новое ПО, которое всё также не удовлетворяло требованиям и имело ряд тех же неисправленных замечаний.** |
| **FireWall/NGFW (Next Generation FireWall)** | В процессе эксплуатации с 2019 года выявлены замечания:<br>• пропадание синхронизации маршрутов OSPF<br>• проблемы активации лицензий и с обновлением ПО и кластеризацией<br>• проблемы с технической поддержкой<br>**Вендор обещает проблемы исправить в «следующем релизе», но требуется чистая установка новой версии.** |
| **Proxy/SWG (Secure Web Gateway)** | На данный момент **ни один российский разработчик не может предоставить готовое решение** по проксированию трафика **для энтерпрайз сегмента** |

# СТАТИСТИЧЕСКИЕ ДАННЫЕ ПО ОТЕЧЕСТВЕННОМУ ПО



**С 2015 г.**

организован процесс импортозамещения

**100 %**

российских решений используется для защиты ЗОКИИ

**97 %**

средств управления ИБ отечественного производства к концу 2023г., в конце 2022г. было 62 %

**79 %**

средств резервного копирования отечественного производства к концу 2023г., в конце 2022г. было было 63 %

**98 %**

средств ИБ импортозамещены к концу 2023г.

**Обладая профессиональной командой, выстроенными процессами отбора и внедрения, всё-таки можно заставить работать «наши» решения**

СИСТЕМНЫЙ ОПЕРАТОР
ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ
RUSSIAN POWER SYSTEM OPERATOR
НАЗВАНИЕ ФИЛИАЛА

# СПАСИБО ЗА ВНИМАНИЕ!

www.so-ups.ru
Официальный сайт

https://t.me/so_ups_official
Официальный телеграм-канал

**Александр Капустин**
АО «СО ЕЭС», Ассоциация «Цифровая энергетика»