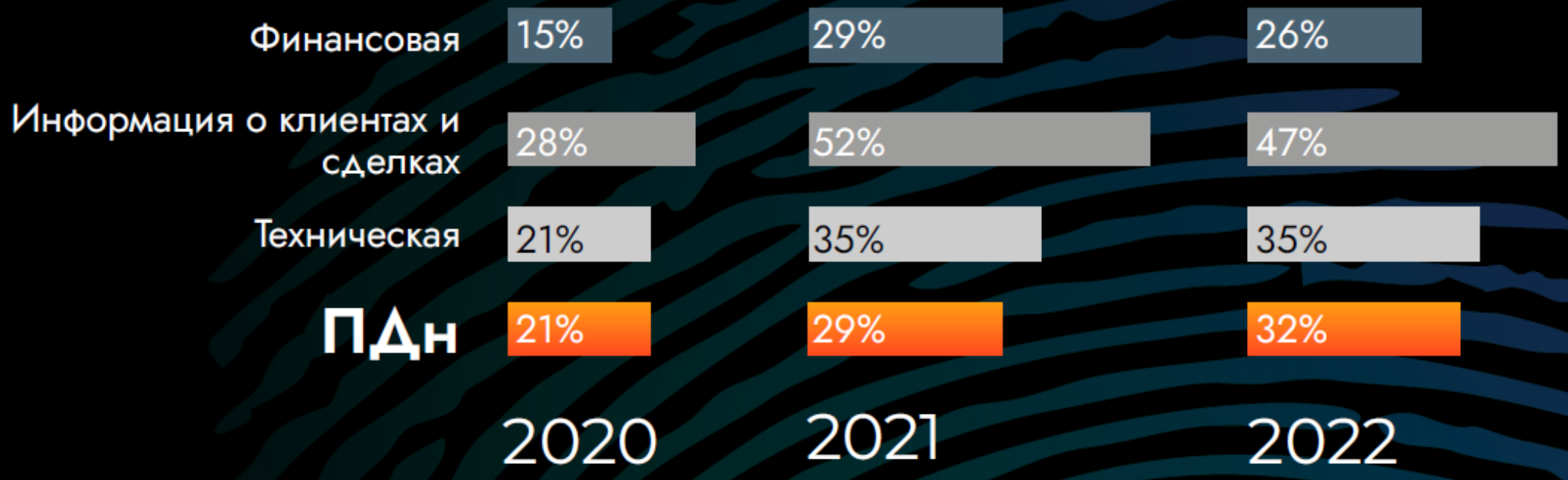
Защита данных нового времени

Алексей Парфентьев

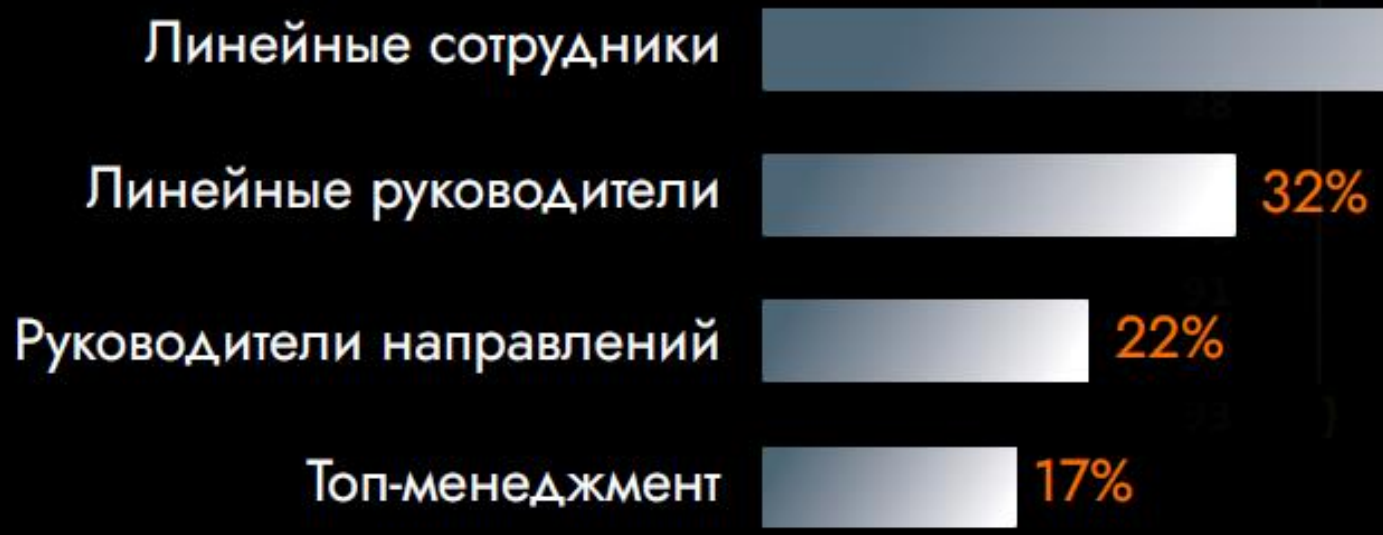
руководитель отдела аналитики «СёрчИнформ»,
руководитель Комитета по ИБ РУССОФТ

SEARCHINFORM
INFORMATION SECURITY

Какая информация утекала из организаций?



Кто чаще становился виновником инцидентов в 2022 г.?*



ИССЛЕДОВАНИЕ УРОВНЯ ИБ В КОМПАНИЯХ РОССИИ ЗА 2022 ГОД

Используемые средства защиты информации:

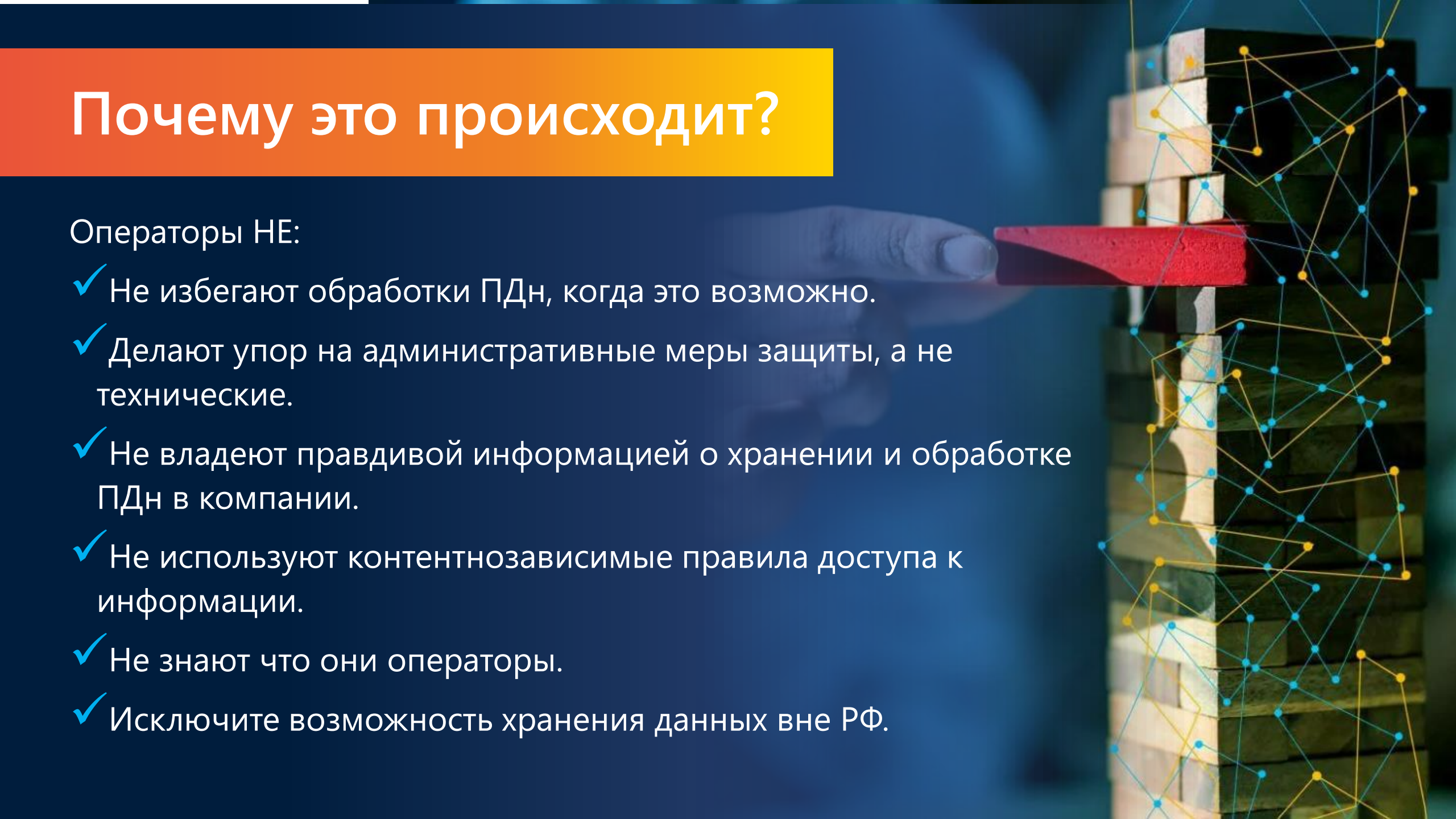
	Госсектор	Частные компании
Антивирус	95%	96%
Средства администрирования Windows	75%	80%
NGFW (Firewall и Proxy)	64%	59%
IDS/IPS/EPS	28%	17%
Шифрование (криптошлюз, ПО)	46%	41%
Контроль целостности	23%	16%
DLP-система	28%	39%
SIEM-система	15%	14%
DCAP-система	1,2%	3%
DAM-решение	1,2%	1%
CASB	1,2%	0,4%

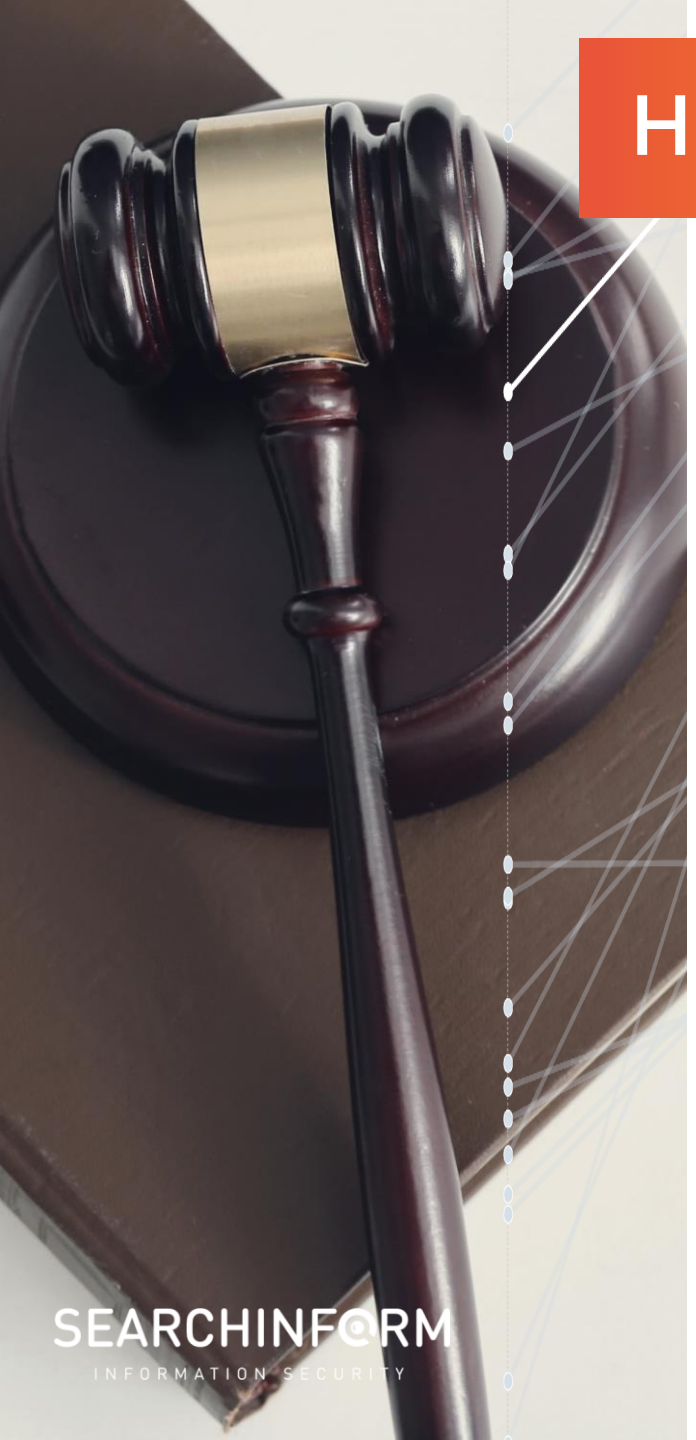
SEARCHINFORM
INFORMATION SECURITY

Почему это происходит?

Операторы НЕ:

- ✓ Не избегают обработки ПДн, когда это возможно.
- ✓ Делают упор на административные меры защиты, а не технические.
- ✓ Не владеют правдивой информацией о хранении и обработке ПДн в компании.
- ✓ Не используют контентнозависимые правила доступа к информации.
- ✓ Не знают что они операторы.
- ✓ Исключите возможность хранения данных вне РФ.





Новинки регулятора. Настоящее и будущее

ВСТУПИЛО В СИЛУ В 2022

- Персональная ответственность руководителя за состояние ИБ в организации (Указ 250)
- Сокращение списка операторов, которые могут НЕ регистрироваться в РКН.
- Необходимость сообщать об инциденте (утечке данных) в течении суток.
- Необходимость предоставлять результаты расследования инцидента в течение трех суток.
- Отмена моратория на проверки

ОЖИДАЕМ В 2023

- Рост размера уголовной и административной ответственности за реализацию ПДн.
- Введение оборотных штрафов за утечки данных.
- ГОСТ по DLP

SEARCHINFORM
INFORMATION SECURITY

Прикладные меры (согласно законодательству)

- Обнаружение фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных.

- Установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе ПДн.

- Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем ПДн.

Прикладные меры (согласно законодательству)

- Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- Отчетность о факте инцидента, предоставление расследования о инциденте (для случая с ПДн и для случая с хакерской атакой).
- Применение средств защиты информации, прошедших в установленном порядке процедуры оценки соответствия.
- При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории РФ.

Необходимый минимум для СЗИ

- **Вести аудит операций с ПДн** (где бы они не хранились) и **прав доступа к ПДн**
- **Проводить инвентаризацию** любых потенциальных мест хранения (используемых, новых, устаревших и любых других)
- Иметь возможность задать **контентно зависимые правила** доступа
- **Быть совместимой** с любой используемой у заказчика ОС
- **Иметь поддержку** облачных хранилищ и сервисов
- Просто **интегрироваться** в общую инфраструктуру средств безопасности (SIEM, DLP, SOC, антивирусы и т.д.)

Прикладные проблемы с отечественным ИБ стеком

- ИБ решение может быть отечественное, но совместимо не со всеми отечественными ОС (правилами Реестра это не запрещено) либо быть спроектировано под Windows.
- ИБ решение может быть отечественное, но в реестре еще не состоять (в частности для СЗИ требуется действующий сертификат ФСТЭК).
- Отечественные СЗИ (сертифицированные) имеют значительную задержку с выпуском обновлений, т.к. каждое обновление проверяется по методике и оформляется во ФСТЭК.
- Отечественные СЗИ потенциально должны поддерживать отечественные CPU
- Решение может быть построено на технологическом стеке Майкрософт и портировать его без потерь функциональности на Linux в принципе невозможно.

Возможные сценарии импортозамещения

Идеалистичный

- Использовать отечественное ПО, оборудование и ПАК. Активно взаимодействовать с разработчиками по ошибкам и доработкам

Реалистичный

- Сильные и конкурентные отечественные решения внедряются и применяются
- Отсутствующие позиции закрываются иностранными как не имеющими аналогов

Дуалистический

- Системное ПО – отечественное на стеке Nix
- Прикладное ПО – отечественное на стеке Nix и MS
- Приклад на MS работает на системном ПО Nix используя технологию динамической интерпретации

Спасибо за внимание!
Вопросы?

https://t.me/
searchinform

https://vk.com/sec
urityinform

https://www.youtube.
com/user/SearchInform

Практика и аналитика