INFOWATCH®

Вопросы, возникающие при сертификации СЗИ по требованиям безопасности информации ФСТЭК России

Андрей Арефьев

Директор по инновационным проектам, InfoWatch

Andrey.Arefiev@infowatch.com

Москва, 2020

Как выбрать сертифицированное решение: на примере DLP-системы

INFOWATCH®

1

Вопрос цены

2

А что там на самом деле сертифицировано?

3

Соответствие потребностей заказчика и деталей, указанных в сертификате

InfoWatch: защита от современных угроз

Безопасность приложений	Безопасность данных и анализ информационных потоков	Безопасность критической информационной инфраструктуры
InfoWatch Attack Killer Защита веб-приложений от хакерских атак	**InfoWatch Traffic Monitor** Контроль и анализ информационных потоков и защита от утечек данных	**InfoWatch ARMA** Защита автоматизированных систем управления технологическими процессами (АСУТП) от кибератак
InfoWatch Appercut Поиск уязвимостей в коде программного обеспечения	**InfoWatch Activity Monitor** Мониторинг действий сотрудников	

InfoWatch: 2000+ выполненных проектов

INFOWATCH®

37 из 50-ти крупнейших компаний РФ

Проекты на сотни тысяч рабочих мест под пристальным вниманием регулятора

InfoWatch: опыт сертификации во ФСТЭК России

- Сертификат соответствия №3205 на **InfoWatch Traffic Monitor:** требования РД НДВ(4) и ТУ
- Сертификат соответствия №3831 на **InfoWatch Traffic Monitor версия 6:** требования ИТ.СКН.П4.ПЗ, ЗБ, РД СВТ (5)
- Сертификат соответствия № 4206 на **InfoWatch Person Monitor:** требования РД НДВ (4) и ТУ
- Сертификат соответствия № 3397 на **Appercut Custom Code Scanner Enterprise Professional версия 4:** требования РД НДВ(4) и ТУ
- **Больше сертификатов в 2020...**

Сертификация для нас — это встроенный процесс при создании продукта

InfoWatch: лицензии ФСТЭК России

- **На деятельность по разработке и производству средств защиты конфиденциальной информации**

  Лицензия ФСТЭК № 0166 от 13 сентября 2004, бессрочная

- **На деятельность по технической защите конфиденциальной информации**

  Лицензия ФСТЭК № 0261 от 13 сентября 2004, бессрочная

Почему важно обращать внимание на наличие лицензий?

Сертификация влияет на стоимость решения. Это нормально.

1	Выделение группы сотрудников, отвечающей за сертификацию
2	Изменение процессов разработки и сопровождения
3	Покупка и внедрение средств, необходимых для обеспечения процессов
4	Проведение испытаний в лаборатории
5	Прохождение экспертизы в органе сертификации
6	Управление уязвимостями
7	Выпуск обновлений
8	Прохождение инспекционного контроля

Сертификация влияет на стоимость решения. Это нормально.

INFOWATCH®

Построение SDLC

1	Управление требованиями (Gira)
2	Управление документацией (confluence)
3	Система контроля исходного кода (git)
4	Статический анализ (**внедряется,** пока без блокировки)
5	Автоматическая сборка
6	Автоматическое тестирование
7	Fuzzing (**внедряется**)
8	Автоматическое VULN-тестирование (внедрение в планах)

- Сертификация влияет на стоимость решения. Это нормально.

INFOWATCH®

Используемые инструменты анализа

Статический	▶ Appercut | infowatch.ru/products/appercut ▶ CLang | clang.llvm.org/cxx_status.html ▶ Cppcheck | cppcheck.sourceforge.net ▶ AppChecker | npo-echelon.ru/production/65/10920
Fuzzing	▶ afl | github.com/google/AFL ▶ gramfuzz | github.com/d0c-s4vage/gramfuzz

Сертификация влияет на стоимость решения. Это нормально.

INFOWATCH®

Разработка математической модели

Вариант № 1

- Написать самим
- Формализовать и верифицировать
- **От 6 месяцев…**

Вариант №2

- Использовать функционал сертифицированной OS

```
bool accepts(⟨Σ, Q, s, T, δ⟩ : Automaton, w:
  R_0 = {s}
  for i = 1 to w.length
     R_i = ∅
     for (q in R_{i-1})
        R_i = R_i ∪ δ(q, w[i])
  return R_|w| ∩ T ≠ ∅
```

ASTRALINUX® special edition

INFOWATCH®

А что там на самом деле сертифицировано?

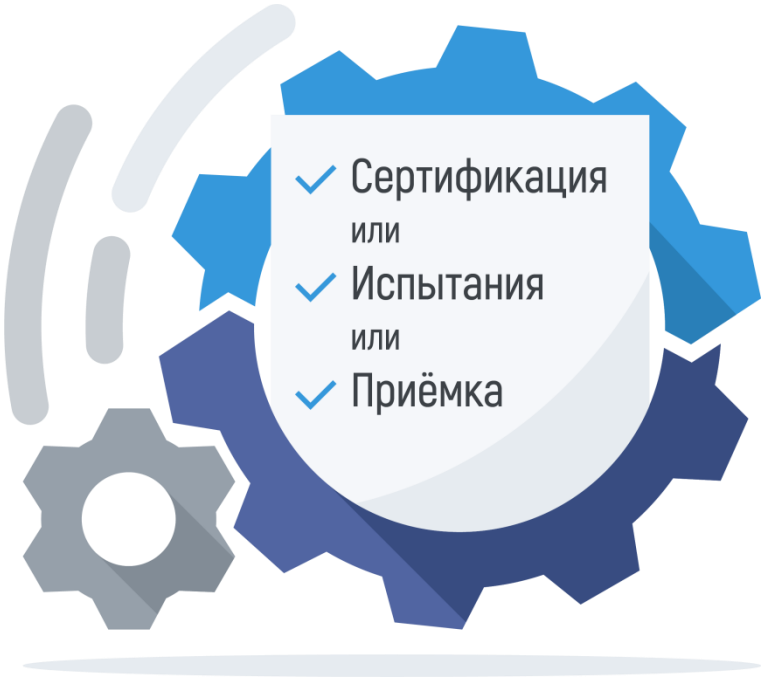
Стыкуем потребности в сертифицированном решении и детали сертификатов

Кому нужна сертифицированная DLP

INFOWATCH®

1. Вы работаете с государственной тайной или вы — ГИС

- Приказ ФСТЭК России № 17



2. Во всех остальных случаях требуется оценка соответствия:

- Приказ ФСТЭК России № 21
- Приказ ФСТЭК России № 31
- Приказы ФСТЭК России № 235 и 239

Меры, закрываемые DLP: Приказ № 17

IV. Защита машинных носителей информации (ЗНИ)

ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации
ЗНИ.7	Контроль подключения машинных носителей информации

Меры, закрываемые DLP: Приказ № 17

INFOWATCH®

XIII. Защита информационной системы, её средств, систем связи и передачи данных (ЗИС)

ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя

Меры, закрываемые DLP: Приказ № 21

IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)

ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещённой к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях

Меры, закрываемые DLP: Приказ № 21

INFOWATCH®

XIII. Защита информационной системы, её средств

ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя

Меры, закрываемые DLP: Приказ № 31

INFOWATCH®

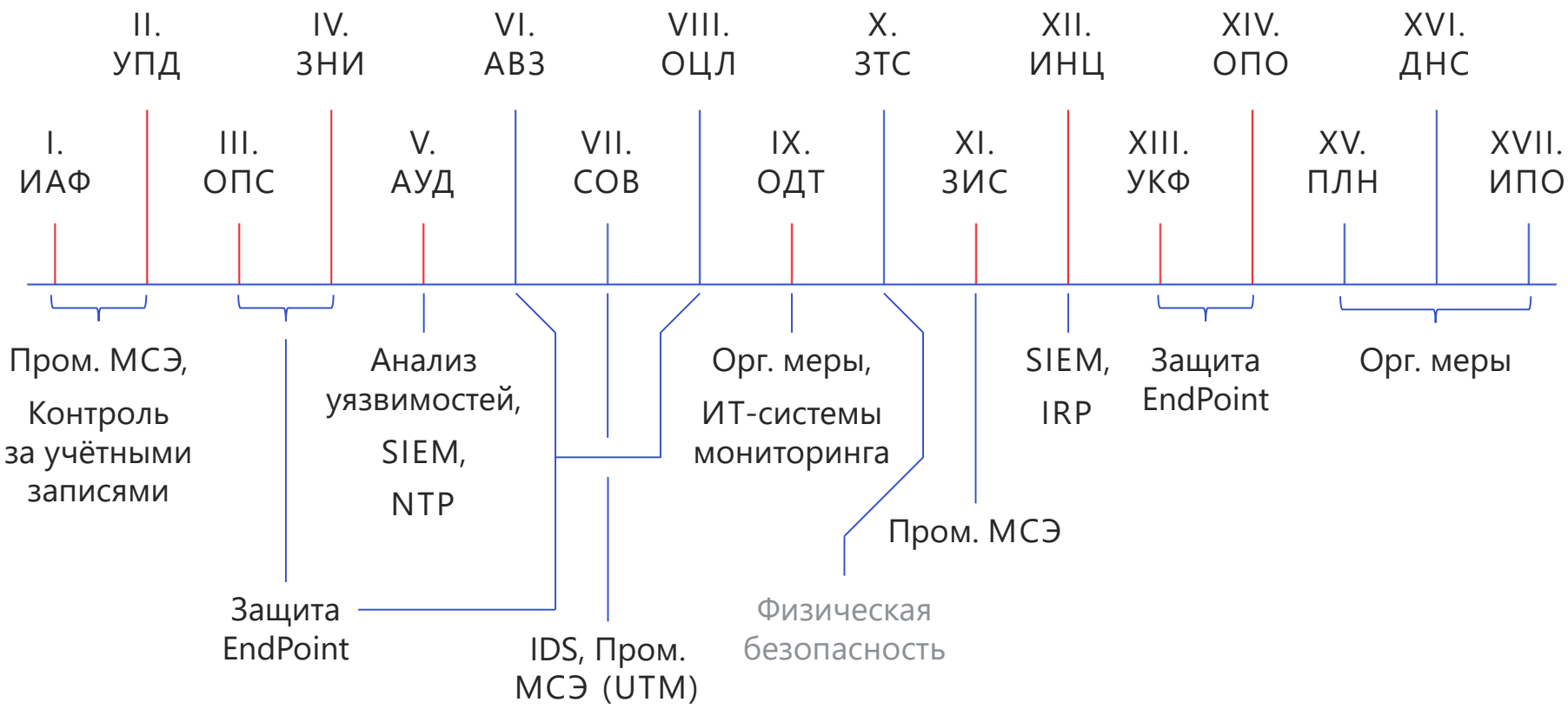
IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации
ЗНИ.7	Контроль подключения машинных носителей информации
V. Аудит безопасности (АУД)	
АУД.9	Анализ действий пользователей
АУД.10	Проведение внутренних аудитов

Меры, закрываемые DLP: Приказ № 31

INFOWATCH®

XI. Защита информационной (автоматизированной) системы и её компонентов (ЗИС)	
ЗИС.17	Защита информации от утечек
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещённых к использованию
ЗИС.26	Подтверждение происхождения источника информации
ЗИС.28	Исключение возможности отрицания отправки информации
ЗИС.29	Исключение возможности отрицания получения информации

Меры, закрываемые промышленным МЭ: Приказ № 239



Возьмите на стенде А45

Выбор критериев сертификации: ключевые детали

INFOWATCH®

Нормативная база с неоднозначным прочтением

- Руководящий документ по уровням доверия, на замену 3-й части ГОСТ 15408, пересекаются с ГОСТ Р 56939-2016
- ГОСТ Р 56939-2016 (SDL: Общие требования)
- ГОСТ Р 58412-2019 (SDL: предотвращением появления и / или устранением уязвимостей программ)
- ГОСТ 15408 (Общие критерии к уровням доверия СЗИ)
- ГОСТ ЕСПД (Документирование ПО — с 70-х)

Профили DLP не утверждены. Но есть проекты.

Сертификация до 2020 года и после

INFOWATCH®

До 2016

По НДВ 4 + ТУ + задание по безопасности*

2016–2019

По профилю защиты средств контроля подключения съёмных машинных носителей информации четвёртого класса защиты ИТ.СКН.П4.ПЗ. + задание по безопасности

*Задание по безопасности подготовлено на основе функциональных требований из неутверждённого профиля DLP

Выбор уровня сертификации на примере InfoWatch Traffic Monitor

Соответствие требованиям:

- Профиля защиты средств контроля подключения съёмных машинных носителей информации четвёртого класса защиты ИТ.СКН.П4.ПЗ.
- Руководящего документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России 2018 г.) по 4 уровню доверия
- Заданию по безопасности

Профиль DLP не утверждён, руководящий документ частично покрывает функционал типовой DLP

Руководствуемся принципом баланса при выборе объекта оценки

Для вендора	Найти баланс между сложностью сертификации и потребностями клиентов
Для клиента	Понимать, что в действительности сертифицировано и каким задачам отвечает

А пока в поисках баланса…

- Минимизируем интеграции со сторонним ПО, облачными сервисами
- Отказываемся от использования: Kubernetes, Docker, Flannel
- Явно выделяем из объекта оценки OS,DB и др.

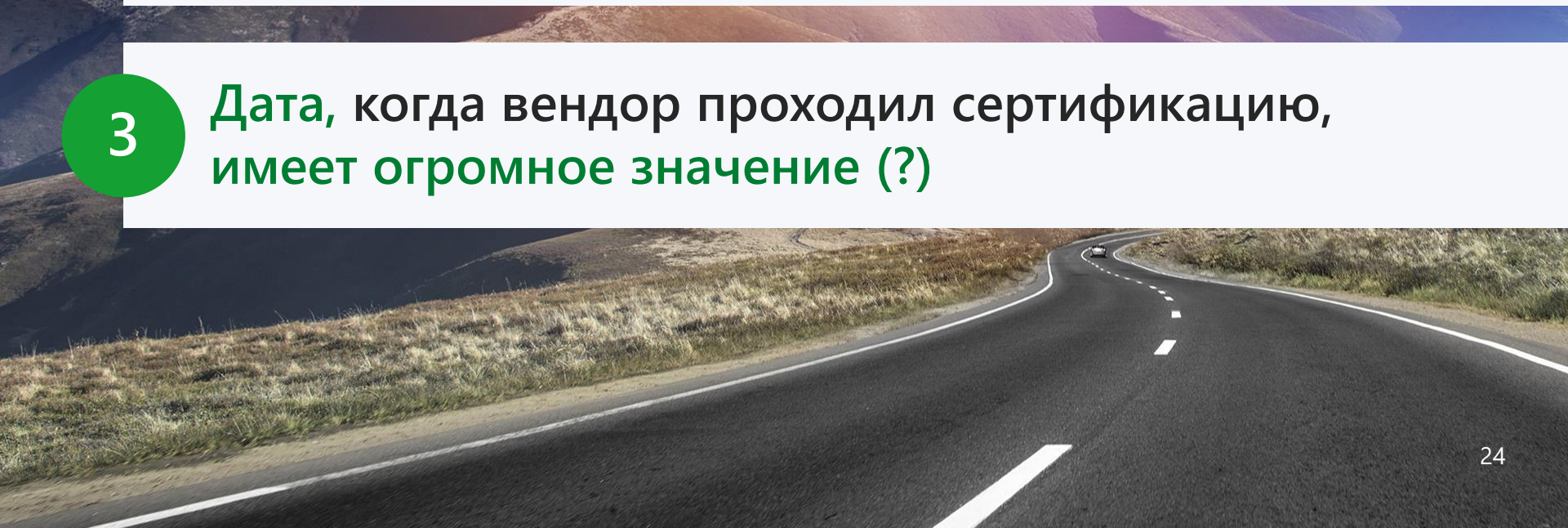
Памятка: выбор сертифицированного решения на примере DLP

INFOWATCH®

1. **Сертификация — гарантия качества,** которая отражается на стоимости продукта

2. **Проверяйте, каким именно задачам** соответствует заявленный сертификат

3. **Дата,** когда вендор проходил сертификацию, **имеет огромное значение (?)**



INFOWATCH®

Приглашаем к обсуждению: стенд A45

Андрей Арефьев

Директор по инновационным проектам, InfoWatch

Andrey.Arefiev@infowatch.com

/InfoWatchOut

infowatch.ru

/InfoWatch