Как выбрать средства защиты от несанкционированного доступа

Илья Шабанов
Генеральный директор
Anti-Malware.ru

Специфика рынка СЗИ от НСД

Специализированные наложенные средства защиты информации от несанкционированного доступа (СЗИ от НСД)

Рынок уходит корнями в 90-е годы

- Требование руководящих документов Гостехкомиссии
- Создавался в качестве усиления встроенных в ОС средств защиты
- Навязывается ФСТЭК России как обязательный элемент защиты ПДн, ГИС
- **На рынке только российские производители!**

Драйверы рынка

- ФЗ № 152-ФЗ от 27 июля 2006 г. «О персональных данных»
- Закон Российской Федерации № 5485-I «О государственной тайне» от 21 июля 1993 г.
- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в ГИС»
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21
- Приказ ФСТЭК России от 14 марта 2014 г. № 31

Без требований ФСТЭК рынка СЗИ от НСД не будет

Требования ФСТЭК России

- РД СВТ, Гостехкомиссия России, 1992 г.
- РД НДВ, Гостехкомиссия России, 1992 г.
- Требования к средствам контроля съемных машинных носителей информации, приказ ФСТЭК № 87
- Требования к межсетевым экранам, приказ ФСТЭК № 9
- Требования к системам обнаружения вторжений, приказ ФСТЭК № 638
- Требования к средствам антивирусной защиты, приказ ФСТЭК № 28

ANTI-MALWARE

Защитные механизмы

- Идентификация и аутентификация пользователей
- Дискреционный контроль доступа пользователей
- Мандатный контроль доступа пользователей и процессов
- Маркировка документов и контроль их вывода на печать
- Защита ввода и вывода информации на отчуждаемый физический носитель
- Регистрация событий безопасности в журнале событий
- Контроль целостности критичных файлов и данных
- Контроль доступа к периферийным устройствам и портам ввода-вывода
- Гарантированное удаление данных на дисках

Российские продукты

КОД БЕЗОПАСНОСТИ

ОКБ АПР

КОНФИДЕНТ CONFIDENT

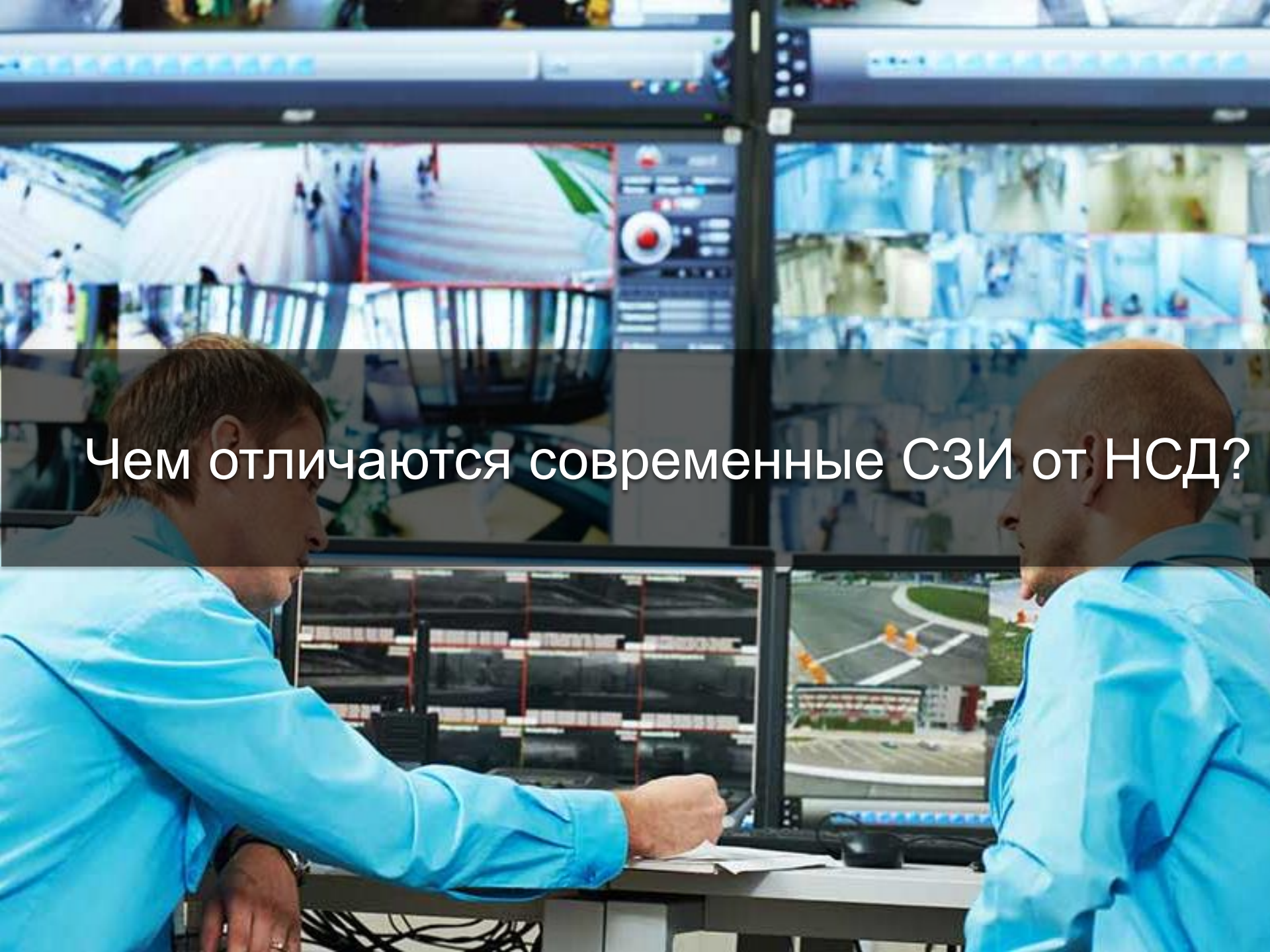
GiS ГАЗИНФОРМСЕРВИС

TSS

ИБ информационная безопасность

РУБИНТЕХ технологии информационной безопасности

Обзор рынка СЗИ от НСД в России https://www.anti-malware.ru/analytics/Market_Analysis/certified-unauthorized-access-security



Чем отличаются современные СЗИ от НСД?

Первое публичное сравнение

- Аккорд-Win64 К (ОКБ САПР)
- Блокхост-Сеть и Блокхост-АМДЗ (Газинформсервис)
- Dallas Lock 8.0-К (Конфидент)
- Diamond ACS (ТСС)
- Панцирь+ (НПП ИТБ)
- Secret Net Studio (Код Безопасности)
- Страж NT 4.0 (Рубинтех)

«Сравнение сертифицированных средств защиты информации от несанкционированного доступа для серверов и рабочих станций (СЗИ от НСД)», Anti-Malware.ru, 2019

Первое публичное сравнение

7 сертифицированных продуктов, более 200 критериев

- Архитектура
- Системные требования
- Уровень сертификации по требованиям ФСТЭК
- Контролируемые объекты
- Контроль целостности
- Замкнутая (изолированная) программная среда
- Контроль портов ввода/вывода и подключаемых устройств
- Контроль подключения внешних устройств
- Контроль печати
- Дискреционное управление достуг
- Мандатное разграничение доступа

Параметр сравнения	Secret Net Studio	Dallas Lock	Аккорд-Win64 K	Блокх
Персональный межсетевой экран (МЭ)				
Фильтрация на сетевом уровне с независимым принятием решений по каждому пакету	Да	Да	Нет	
Фильтрация пакетов служебных протоколов (ICMP, IGMP и т. д.), необходимых для диагностики и управления работой сетевых устройств	Да	Да	Нет	
Фильтрация с учетом входного и выходного сетевого интерфейса для проверки подлинности сетевых адресов	Да	Да	Нет	
Фильтрация на транспортном уровне запросов на установление виртуальных соединений (TCP-сессий)	Да	Да	Нет	
Фильтрация на прикладном уровне запросов к прикладным сервисам (фильтрация по символьной	Да	Да	Нет	

«Сравнение сертифицированных (СЗИ от НСД)», Anti-Malware.ru, 2019

Уровень сертификации ФСТЭК

	Secret Net Studio	Dallas Lock 8.0-K	Аккорд-Win64 К	Блокхост-Сеть	КСЗИ Панцирь+	Diamond ACS	Страж NT
РД СВТ	5 класс СВТ от НСД	5 класс СВТ от НСД	5 класс СВТ от НСД	3 класс СВТ от НСД	5 класс СВТ от НСД	3 класс СВТ от НСД	3 класс СВТ от НСД
РД НДВ	НДВ 4	НДВ 4	НДВ 4	НДВ 2	НДВ 4	НДВ 2	НДВ 2
МЭ РД	Нет	Нет	Нет	4 класс	4 класс	Нет	Нет
МЭ	4 класс защиты МЭ	4 класс защиты МЭ	Нет	Нет	Нет	Нет	Нет
СКН	4 класс защиты СКН	4 класс защиты СКН	4 класс защиты СКН	Нет	Нет	Нет	Нет
САВЗ	4 класс защиты САВЗ	Нет	Нет	Нет	На ТУ	Нет	Нет
СОВ	4 класс защиты СОВ	4 класс защиты СОВ	Нет	Нет	Нет	Нет	Нет

«Сравнение сертифицированных (СЗИ от НСД)», Anti-Malware.ru, 2019

На что смотреть при выборе?

- Какой уровень сертификации необходим
- Какие версии Windows используется (10 и Server 2016 поддерживаются не у всех)
- С какими токенами нужна совместимость
- Какой нужен набор дополнительных модулей
- Какие требования к управлению и отчетности

Это значительно сократит выбор оптимальной системы

Итоги сравнения

- ПАК только у Diamond ACS
- Сервера безопасности Стража, у Аккорда доп. продукт
- Сильно разная поддержка токенов и смарт-карт
- Контроль целостности системы лучше всего реализован в SNS, Dallas Lock и Аккорд-Win64
- Изолированная программная среда у всех кроме Diamond ACS
- Теневое копирование информации, выводимой на внешние носители есть в SNS, Dallas Lock и Панцирь+
- В Diamond ACS и Панцирь+ слабо развит контроль печати

Итоги сравнения

- Мандатное разграничение доступа лучше всего реализовано в SNS, Dallas Lock и Аккорд и Diamond ACS
- МЭ есть только в SNS, Dallas Lock, Блокхост и Панцирь+
- СОВ есть только в SNS, Dallas Lock
- САВЗ есть только в SNS
- У Стража плохо развиты групповые политики и отчетность
- Открытый API есть только в SNS, Страже и Блокхост
- Стоимость отличается на 20-25%

Выводы

- Высокая конкуренция на рынке
- Различный уровень сертификации
- Много нюансов реализации одинаковых функций
- Дополнительная функциональность сильно отличается:
  - МЭ
  - СОВ
  - САВЗ
- Наблюдается пересечение с продуктами для защиты конечных точек (Endpoint Security) и агентским DLP

Контакты

Илья Шабанов

Генеральный директор
ilya.shabanov@anti-malware.ru

www.anti-malware.ru

@anti_malware

@Anti_Malware

antimalwareru