Реализация комплексного подхода к учету и контролю машинных носителей информации, включая контроль их перемещения за пределы контролируемой зоны

Сергей Панасенко, компания «Актив», panasenko@guardant.ru

Дмитрий Дударев, Фирма «АНКАД», dudarev@ancud.ru

Нормативная база

- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 (требования по защите информации в государственных информационных системах).
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 (информационные системы персональных данных).
- Приказ ФСТЭК России от 14 марта 2014 г. № 31 (автоматизированные системы управления производственными и технологическими процессами).
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239 (объекты критической информационной инфраструктуры).

Меры защиты информации в части МНИ

ЗНИ.0
Разработка политики защиты машинных носителей информации

ЗНИ.1
Учет машинных носителей информации

ЗНИ.2
Управление доступом к машинным носителям информации

ЗНИ.3
Контроль перемещения машинных носителей информации за пределы контролируемой зоны

ЗНИ.4*
Исключение возможности… использования носителей информации в иных информационных системах

ЗНИ.7
Контроль подключения машинных носителей информации

Вхождение в базовые наборы мер ЗИ

Мера ЗИ	Приказ № 17			Приказ № 21				Приказ № 31			Приказ № 239		
	Классы защищенности ИС			Уровни защищенности ПДн				Классы защищенности АСУ			Категория значимости объекта		
	3	2	1	4	3	2	1	3	2	1	3	2	1
ЗНИ.0	Нет			Нет				+	+	+	+	+	+
ЗНИ.1	+	+	+			+	+	+	+	+	+	+	+
ЗНИ.2	+	+	+			+	+	+	+	+	+	+	+
ЗНИ.3													
ЗНИ.4*								Нет*			Нет*		
ЗНИ.7								+	+	+	+	+	+

Сложность реализации ЗНИ.3

Реализация контроля перемещения МНИ за пределы контролируемой зоны по периметру КЗ затруднена и требует применения различных организационных мер, например:

1 **Организация досмотра по периметру КЗ**

2 **Противовес тенденции на миниатюризацию носителей:**

- запрет на использование МНИ меньше определенного размера в ИС
- принудительное увеличение размера и улучшение детектируемости МНИ (коробы, радиометки и т.п.)

Общий принцип:

сложно доказать отсутствие чего-либо где-либо (МНИ за пределами КЗ); значительно проще доказать наличие конкретного предмета в определенном месте (МНИ в конкретном месте внутри КЗ)

Альтернатива: «белый список» разрешенных мест нахождения МНИ

Основная идея:

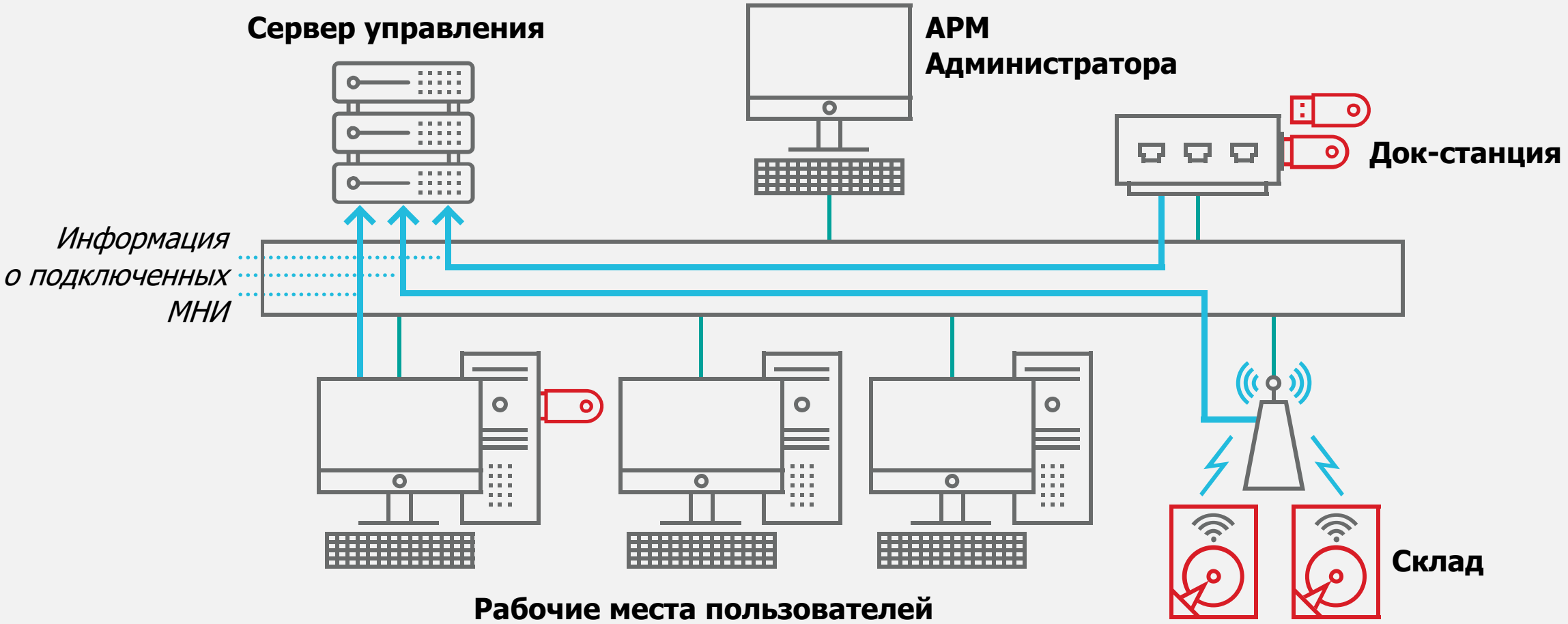
вместо контроля пересечения периметра КЗ осуществляется контроль местонахождения МНИ в пределах КЗ

Каждый зарегистрированный (отслеживаемый) МНИ должен находиться в одном из разрешенных местоположений (например, АРМ пользователя или док-станция/склад)

Допускается отсутствие МНИ в разрешенном местоположении в пределах таймаута (для переноса МНИ из одного разрешенного места в другое)

Отсутствие свыше таймаута – событие информационной безопасности

Распределенная клиент-серверная система наблюдения
за местоположением МНИ



Распределенная клиент-серверная система наблюдения за местоположением МНИ

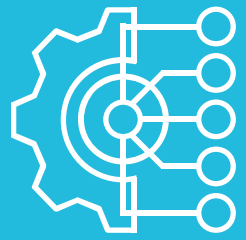
ПО клиента устанавливается в разрешенных местоположениях и отслеживает подключение носителей

АРМ Администратора, на котором выполняется настройка системы, администрирование носителей, отслеживание местонахождения МНИ и событий в реальном времени и т. п.

Сервер собирает информацию от клиентов и обрабатывает ее (в частности, отслеживает наличие всех носителей и таймауты периодов отсутствия, генерирует события безопасности)

ПО клиента устанавливается также в месте сбора (сдачи) неиспользуемых носителей (склад, док-станция…)

Дополнительные возможности



- Контроль может осуществляться как по физическому подключению носителей (например, USB), так и бесконтактным образом (например, с помощью оснащения МНИ RFID-метками)
- Подмножество разрешенных местоположений, величины таймаутов, реакции на события могут быть настроены для каждого носителя индивидуально
- Местоположение МНИ может отображаться в режиме реального времени
- На основе системы может быть построен полнофункциональный комплекс управления носителями

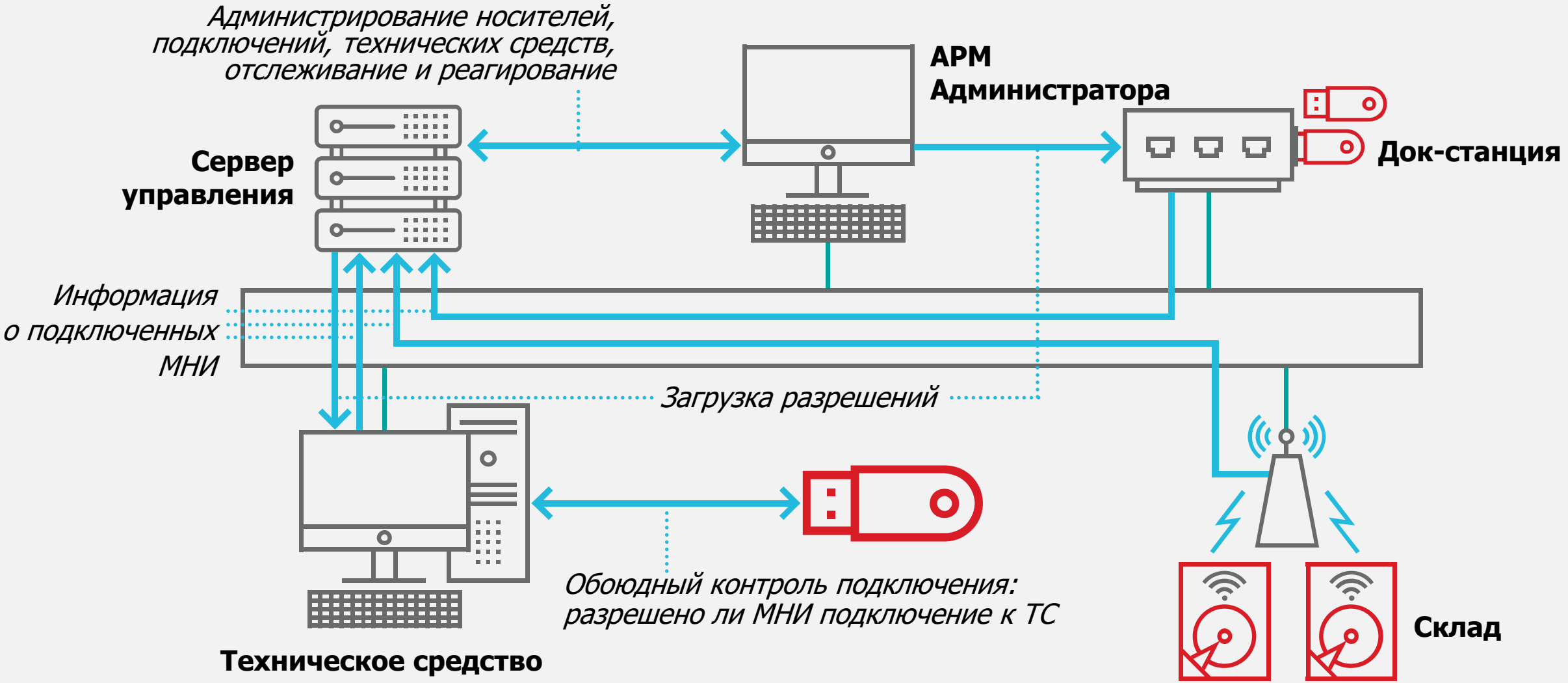
Дополнительные меры контроля

Клиентское ПО может включать в себя второй «белый список», ограничивающий подключение к компьютеру (на котором оно установлено) носителей только перечнем разрешенных

Носители могут быть специальными, в этом случае каждый носитель может иметь третий «белый список» – перечень компьютеров (например, определяемых по идентификаторам установленных на них модулей доверенной загрузки), к которым носитель может подключаться, а также контролировать подключения в соответствии с данным перечнем

Расширение на аутентифици-рующие носители

Схема комплекса управления МНИ



Описание комплекса управления МНИ

1 **ПО клиента:**
контролирует подключения МНИ и передает информацию о них

2 **Сервер управляет всеми аспектами работы с МНИ:**

- списки ТС и МНИ, разрешения на подключение для ТС и МНИ, разрешенные местонахождения МНИ и таймауты
- загрузка списков разрешений на ТС
- сбор данных и отслеживание подключений, местонахождения, таймаутов
- генерация событий безопасности

3 **АРМ Администратора:**

- администрирование всех списков
- загрузка списков разрешений на МНИ
- отслеживание местонахождения МНИ и событий в реальном времени

Комплекс частично реализует дополнительные меры ЗИ

ИАФ.4

Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

УПД.15

Регламентация и контроль использования в информационной системе мобильных технических средств

ЗНИ.4**

Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях

Вхождение в базовые наборы мер ЗИ

Мера ЗИ	Приказ № 17			Приказ № 21				Приказ № 31			Приказ № 239		
	Классы защищенности ИС			Уровни защищенности ПДн				Классы защищенности АСУ			Категория значимости объекта		
	3	2	1	4	3	2	1	3	2	1	3	2	1
ИАФ.4	+	+	+	+	+	+	+	+	+	+	+	+	+
УПД.15	+	+	+	+	+	+	+	Нет			Нет		
ЗНИ.4**													

Выводы

Реализация контроля перемещения машинных носителей информации за пределы контролируемой зоны «напрямую» (по периметру КЗ) затруднена; более эффективным выглядит контроль местонахождения внутри КЗ по принципу «белого списка»

Данный контроль может осуществляться в качестве одной из функций комплексной системы регистрации, учета и контроля машинных носителей информации, направленной на реализацию комплекса мер по их защите в соответствии с приказами ФСТЭК России

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

Сергей Панасенко, компания «Актив»,
panasenko@guardant.ru

Дмитрий Дударев, Фирма «АНКАД»,
dudarev@ancud.ru