ViPNet SIES

в разрезе требований Приказа ФСТЭК России №239 от 25.12.17 г.

План вебинара

1

ViPNet SIES - Краткий обзор решения

2

Меры защиты информации согласно Приказу №239 ФСТЭК России

3

Закрытие мер продуктами решения ViPNet SIES согласно Приказу №239 ФСТЭК России

infotecs

ViPNet SIES: краткий обзор

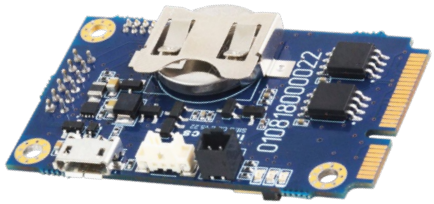
Решение ViPNet SIES

ВСТРАИВАЕМЫЕ КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ИНТЕГРАЦИИ В УСТРОЙСТВА АВТОМАТИЗАЦИИ НА ВСЕХ УРОВНЯХ АСУ

ЗАЩИТА КОММУНИКАЦИЙ • ЗАЩИТА КОНЕЧНЫХ УЗЛОВ • ЗАЩИТА ДАННЫХ • АУТЕНТИФИКАЦИЯ И ИДЕТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

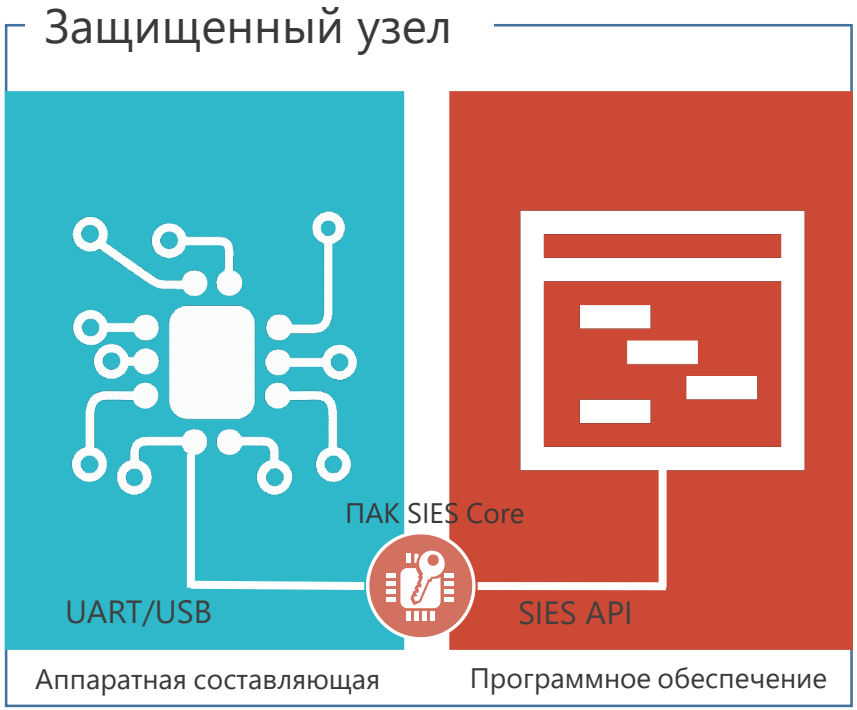
Решение ViPNet SIES

Встраивание продуктов решения ViPNet SIES



ПАК SIES Core

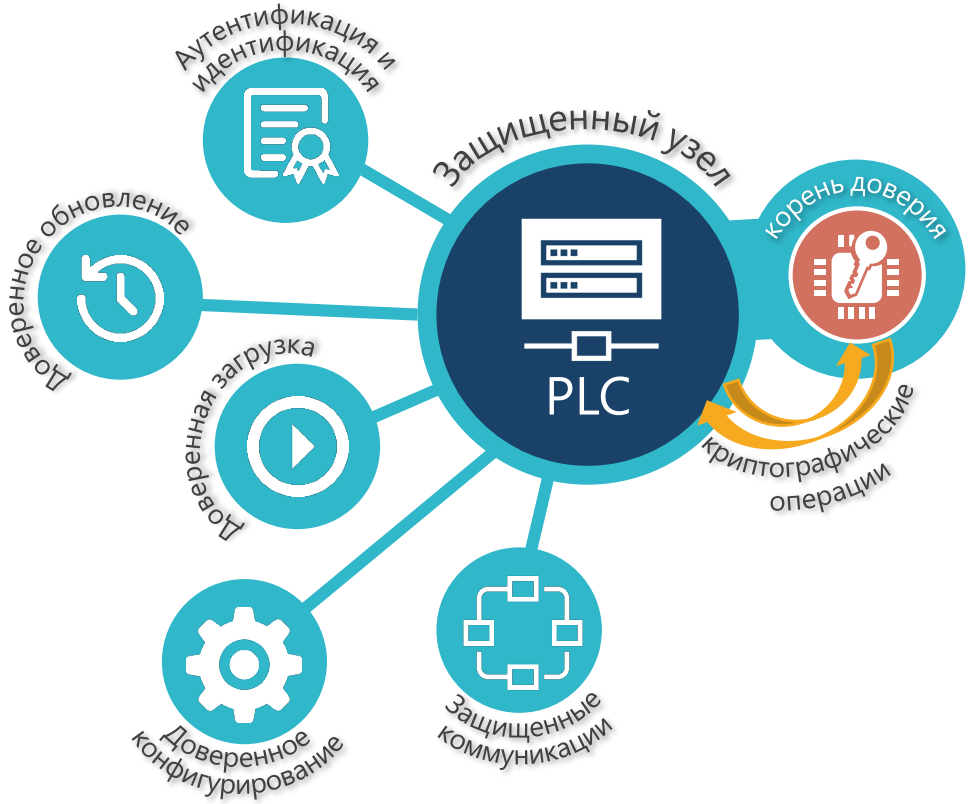
Встраивание продуктов решения ViPNet SIES



Встраивание на аппаратном уровне (только ПАК ViPNet SIES Core):
– интерфейс UART
– интерфейс USB

Встраивание на программном уровне:
– SIES API (Прикладной протокол+ RATP) или SIES SDK для ПАК ViPNet SIES Core
- REST API для ПО ViPNet SIES Unit

Защищенное устройство автоматизации



Криптографические операции:

- Шифрование/расшифрование по CRISP
- Создание имитавставки/проверка имитавставки по CRISP
- Создание ЭП/ проверка ЭП в CMS
- Шифрование/расшифрование в CMS
- Создание хэш/проверка хэш

CRISP

Cryptographic Industrial Security Protocol
- неинтерактивный протокол защищенной передачи данных для индустриальных систем, M2M и IIoT коммуникаций

- Обеспечение целостности
- Обеспечение конфиденциальности (опционально)
- Защита от навязывания повторных сообщений
- Окно принятых сообщений

- Общий секретный ключ
- Защита данных – блочный шифр, имитовставка
- Поддержка адресных (один-к одному) сообщений
- Поддержка многоадресных (один ко многим, подписочная модель) сообщений
- Явная и неявная адресация абонентов

CRISP

C

Минимальные накладные расходы

R

Обеспечение минимальных задержек

I

Работа на плохих каналах связи

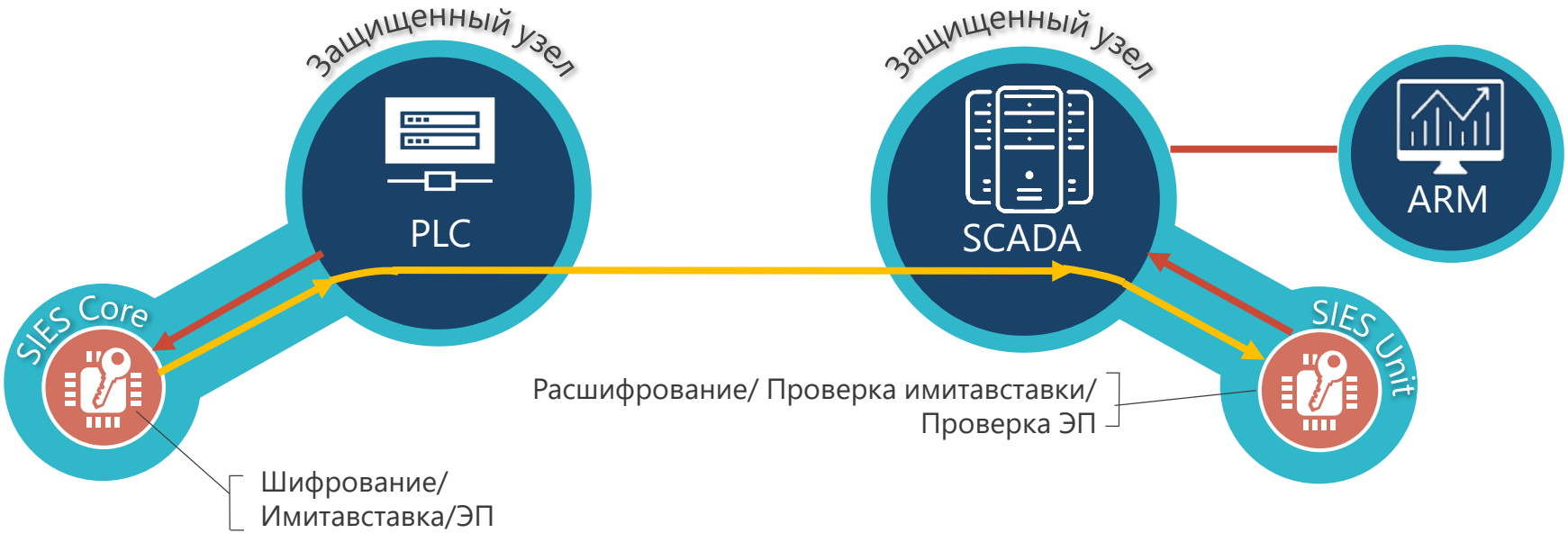
S

Высокая энергоэффек-тивность

P

Отсутствие влияния на доступность

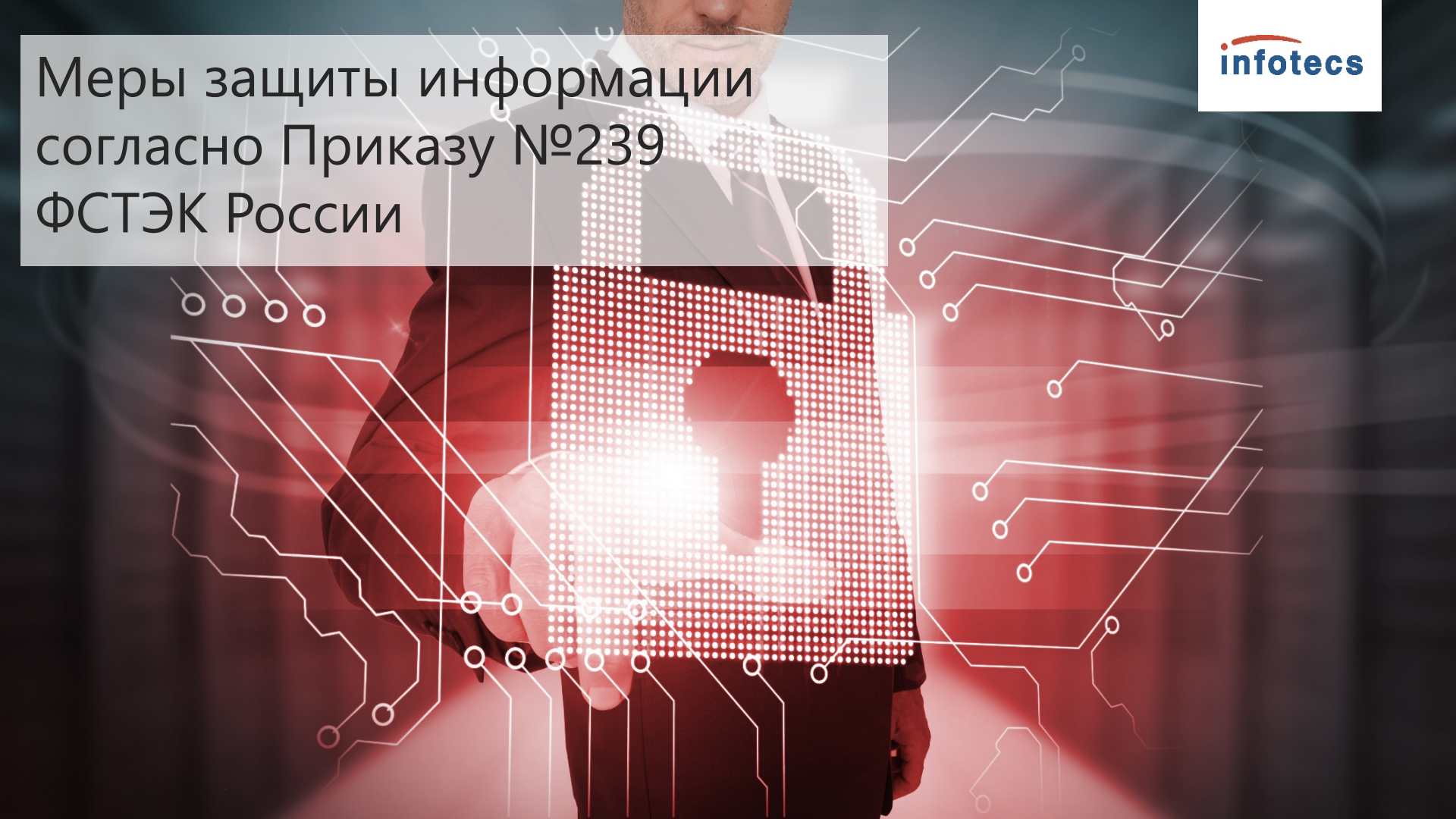
Как это работает



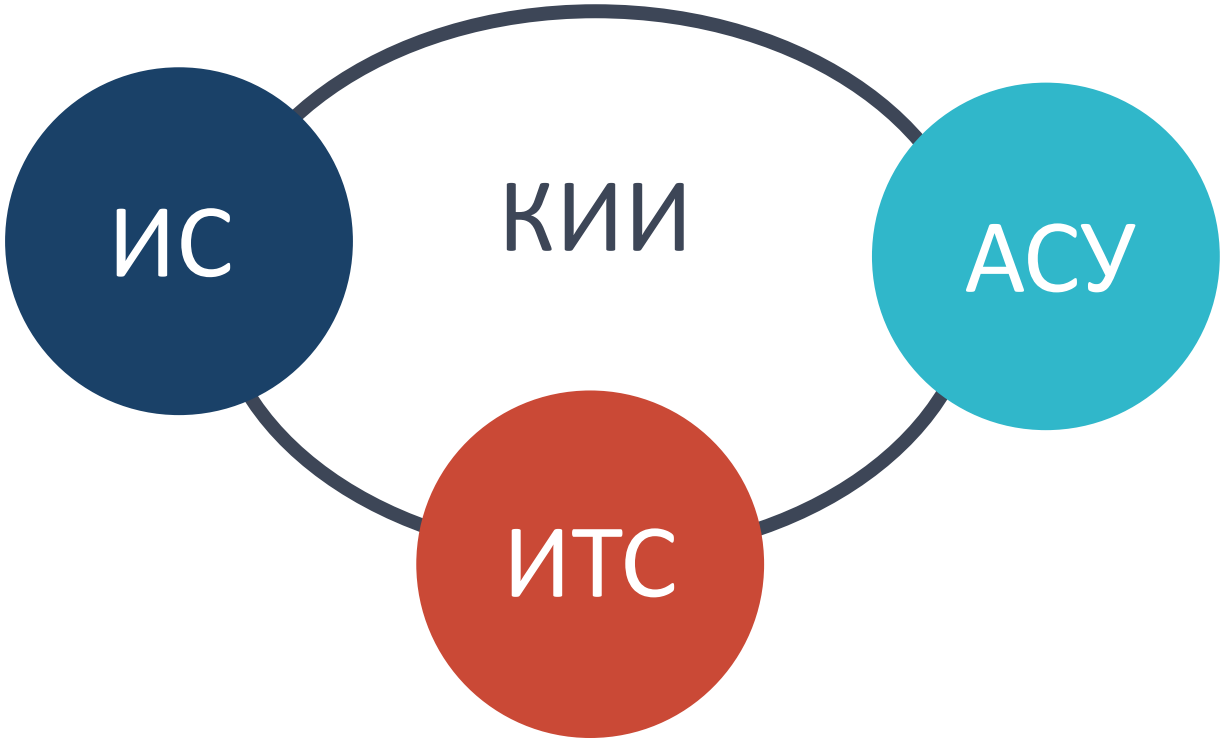
открытые данные

защищенные данные

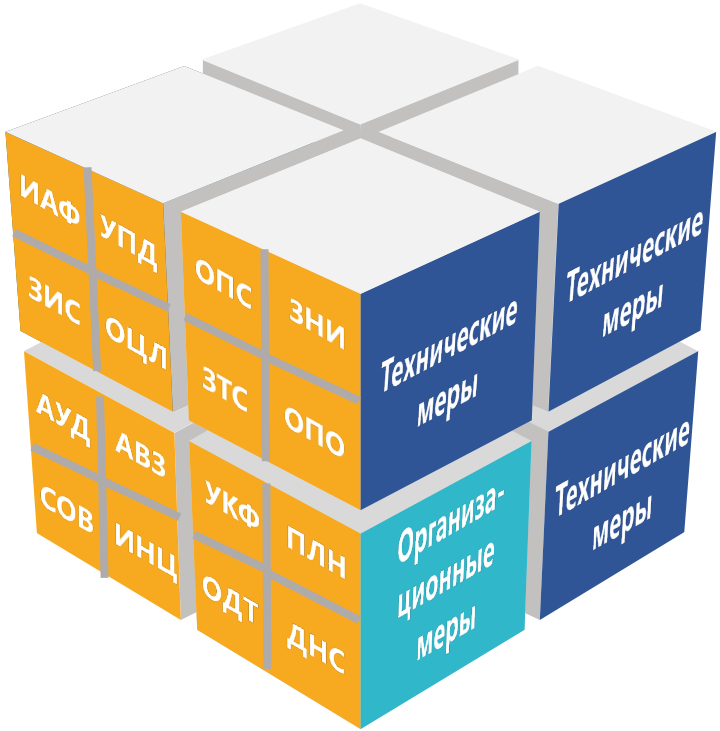
Меры защиты информации согласно Приказу №239 ФСТЭК России



Защита КИИ промышленных предприятий

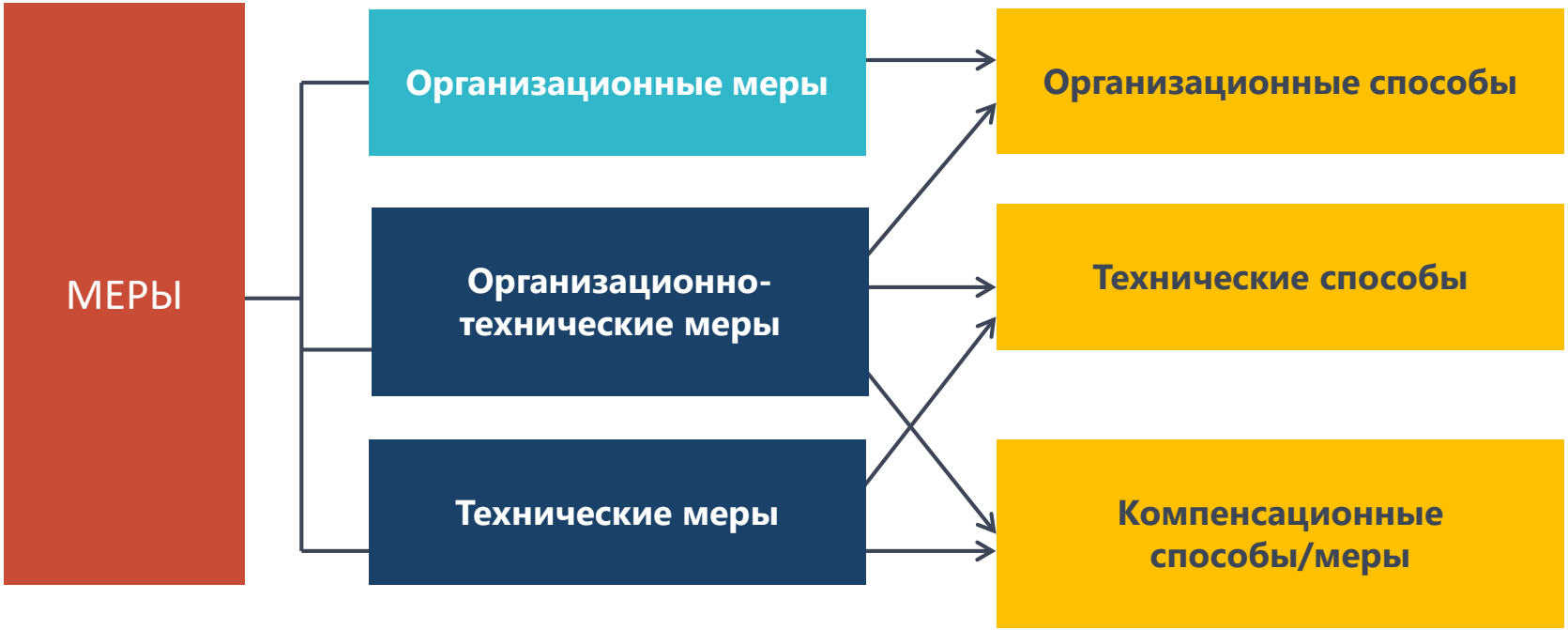


Состав мер по защите объектов КИИ согласно Приказу №239 ФСТЭК России



I. Идентификация и аутентификация (ИАФ)
II. Управление доступом (УПД)
III. Ограничение программной среды (ОПС)
IV. Защита машинных носителей информации (ЗНИ)
V. Аудит безопасности (АУД)
VI. Антивирусная защита (АВЗ)
VII. Предотвращение вторжений (компьютерных атак) (СОВ)
VIII. Обеспечение целостности (ОЦЛ)
IX. Обеспечение доступности (ОДТ)
X. Защита технических средств и систем (ЗТС)
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
XII. Планирование мероприятий по обеспечению безопасности (ПЛН)
XIII. Управление конфигурацией (УКФ)
XIV. Управление обновлениями программного обеспечения (ОПО)
XV. Реагирование на инциденты информационной безопасности (ИНЦ)
XVI. Обеспечение действий в нештатных ситуациях (ДНС)
XVII. Информирование и обучение персонала (ИПО)

Состав мер по защите объектов КИИ согласно Приказу №239 ФСТЭК России



Объекты защиты для АСУ

Информация о параметрах и объектах процесса АСУ

Входная и выходная информация, управляющая информация, контрольно-измерительная информация, иная критическая информация

Программные средства АСУ

Микропрограммное, общесистемное, прикладное программное обеспечение

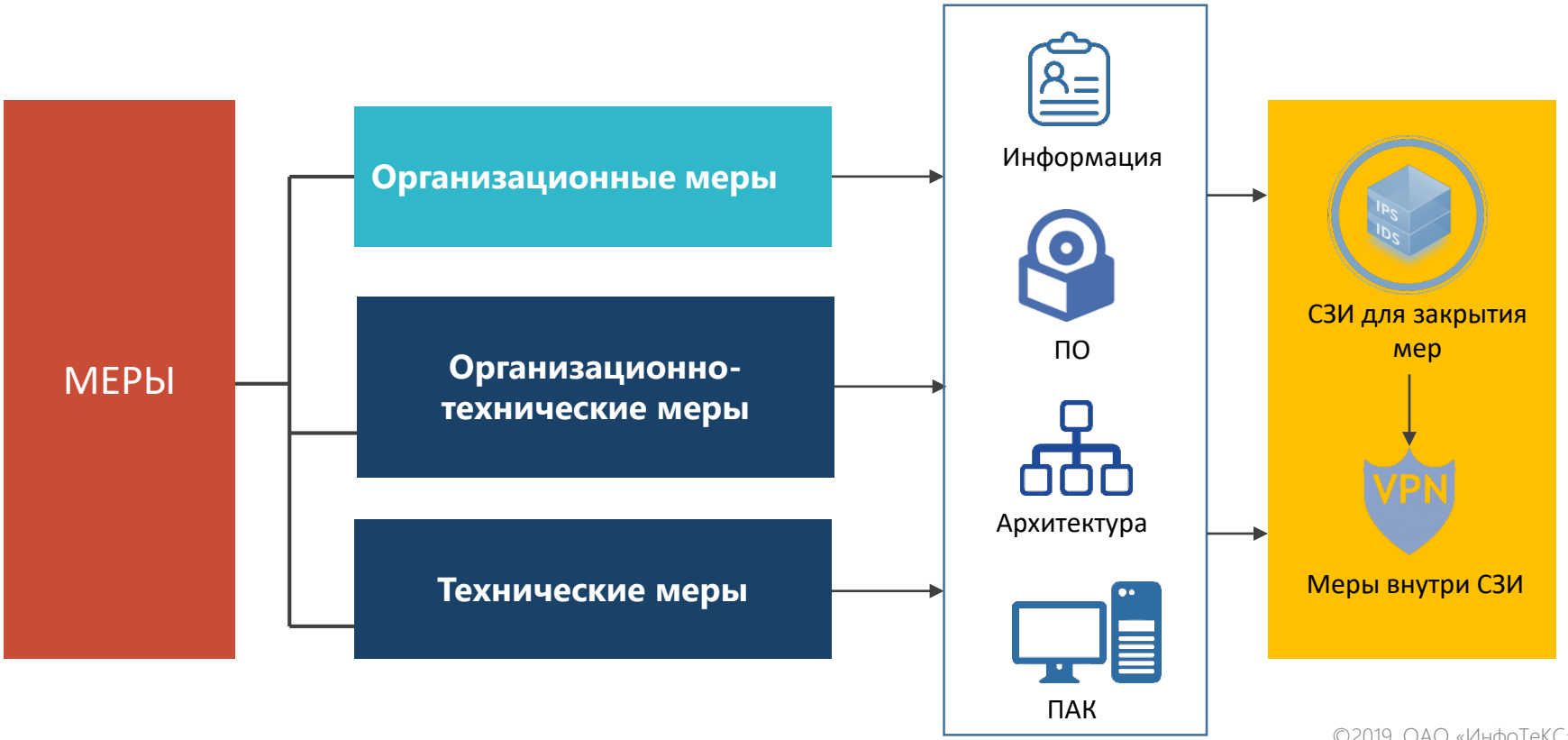
Программно-аппаратные средства АСУ

АРМ, промышленные серверы, телекоммуникационное оборудование, линии связи, ПЛК, производственное и технологическое оборудование, исполнительные устройства

Средства защиты информации

Архитектура и конфигурация АСУ

Меры защиты и объекты защиты



Закрытие мер продуктами решения ViPNet SIES согласно Приказу №239 ФСТЭК России

Меры защиты

Легенда

Название меры	Организационные меры
Название меры	Мера, которую закрывают продукты ViPNet SIES
Название меры	Мера защиты самих продуктов ViPNet SIES

I. Идентификация устройств

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
ИАФ.0	*Разработка политики идентификации и аутентификации*	+	+	+		
ИАФ.1	**Идентификация и аутентификация пользователей и инициируемых ими процессов**	+	+	+	ViPNet SIES Core	• Защищенный доступ к устройству с локальной аутентификацией пользователя • Защищенный доступ к устройству с аутентификацией пользователя удаленного АРМ
ИАФ.2	**Идентификация и аутентификация устройств**	+	+	+	ViPNet SIES Core ViPNet SIES Unit	• Обеспечение конфиденциальности информации • Обеспечение целостности информации • Аутентификацию обеспечивает протокол CRISP
ИАФ.3	**Управление идентификаторами**	+	+	+	ViPNet SIES MC	• Регистрация защищаемых устройств
ИАФ.4	**Управление средствами аутентификации**	+	+	+	ViPNet SIES MC	• Управление ViPNet SIES Core, ViPNet SIES Unit

I. Идентификация устройств

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
ИАФ.5	**Идентификация и аутентификация внешних пользователей**	+	+	+	• ViPNet SIES Core	• Защищенный доступ к индустриальному устройству с локальной аутентификацией пользователя • Защищенный доступ к индустриальному устройству с аутентификацией пользователя удаленного АРМ • Внешнего пользователя нужно предварительно зарегистрировать
ИАФ.6	Двусторонняя аутентификация					
ИАФ.7	**Защита аутентификационной информации при передаче**	+	+	+	ViPNet SIES Core ViPNet SIES Unit	• Обеспечение конфиденциальности информации • Обеспечение целостности информации • Данные сценарии позволяют защитить информацию любого типа

II. Управление доступом

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
УПД.0	*Разработка политики управления доступом*	+	+	+		
УПД.1	**Управление учетными записями пользователей**	+	+	+	ViPNet SIES MC	• Поддержка реализации меры с помощью SIES-узлов другого типа. Мера реализуется на защищаемом устройстве
УПД.2	**Реализация политик управления доступом**	+	+	+	ViPNet SIES MC	• Поддержка реализации меры с помощью регистрации прикладных связей между SIES-узлами. • Мера реализуется на защищаемом устройстве
УПД.3	**Доверенная загрузка**		+	+	ViPNet SIES Core	• Проверка подлинности и аутентичности системного ПО. Мера реализуется на защищаемом устройстве
УПД.4	**Разделение полномочий (ролей) пользователей**	+	+	+	ViPNet SIES MC	• Поддержка реализации меры с помощью регистрации прикладных связей между SIES-узлами. Мера реализуется на защищаемом устройстве

II. Управление доступом

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
УПД.5	Назначение минимально необходимых прав и привилегий	+	+	+		
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+	+	+		
УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам					
УПД.8	Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе			+		
УПД.9	Ограничение числа параллельных сеансов доступа			+		
УПД.10	Блокирование сеанса доступа пользователя при неактивности	+	+	+		

II. Управление доступом

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
УПД.11	Управление действиями пользователей до идентификации и аутентификации	+	+	+		
УПД.12	Управление атрибутами безопасности					
УПД.13	**Реализация защищенного удаленного доступа**	**+**	**+**	**+**	ViPNet SIES Core ViPNet SIES Unit	• Доверенное обновление файла конфигурации технологического процесса • Обеспечение конфиденциальности информации • Обеспечение целостности информации
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+	+	+		

III. Ограничение программной среды

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
ОПС.0	*Разработка политики ограничения программной среды*		+	+		
ОПС.1	**Управление запуском (обращениями) компонентов программного обеспечения**			+	ViPNet SIES Core ViPNet SIES Unit	• Доверенная загрузка приложений/ПО
ОПС.2	**Управление установкой (инсталляцией) компонентов программного обеспечения**		+	+	ViPNet SIES Core ViPNet SIES Unit	• Доверенное обновление • Доверенное обновление файла конфигурации технологического процесса
ОПС.3	Управление временными файлами					

V. Аудит безопасности

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
АУД.0	*Разработка политики аудита безопасности*	+	+	+		
АУД.1	Инвентаризация информационных ресурсов	+	+	+		
АУД.2	Анализ уязвимостей и их устранение	+	+	+		
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+	+	+		
АУД.4	Регистрация событий безопасности	+	+	+	ViPNet SIES Core ViPNet SIES Unit ViPNet SIES MC	
АУД.5	Контроль и анализ сетевого трафика			+		
АУД.6	Защита информации о событиях безопасности	+	+	+	ViPNet SIES Core ViPNet SIES Unit ViPNet SIES MC	

V. Аудит безопасности

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
АУД.7	Мониторинг безопасности	+	+	+		
АУД.8	Реагирование на сбои при регистрации событий безопасности	+	+	+		
АУД.9	*Анализ действий пользователей*			+		
АУД.10	*Проведение внутренних аудитов*	+	+	+		
АУД.11	*Проведение внешних аудитов*			+		

VIII. Обеспечение целостности (ОЦЛ)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
ОЦЛ.0	*Разработка политики обеспечения целостности*	+	+	+		
ОЦЛ.1	**Контроль целостности программного обеспечения**	+	+	+	ViPNet SIES Core ViPNet SIES Unit	• Доверенное обновление ПО защищаемого устройства • Обеспечение целостности информации Внутренний контроль целостности ПО ViPNet SIES Core • Внутренний контроль целостности ПО ViPNet SIES Unit
ОЦЛ.2	**Контроль целостности информации**				ViPNet SIES Core ViPNet SIES Unit	• Обеспечение целостности информации
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему			+	ViPNet SIES MC	
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему		+	+	ViPNet SIES MC	

VIII. Обеспечение целостности (ОЦЛ)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях		+	+	ViPNet SIES MC	
ОЦЛ.6	Обезличивание и (или) деидентификация информации					

IX. Обеспечение доступности

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
ОДТ.0	*Разработка политики обеспечения доступности*	+	+	+		
ОДТ.1	Использование отказоустойчивых технических средств		+	+		
0ДТ.2	Резервирование средств и систем		+	+		
ОДТ.3	Контроль безотказного функционирования средств и систем		+	+		
ОДТ.4	Резервное копирование информации	+	+	+	ViPNet SIES MC	
ОДТ.5	Обеспечение возможности восстановления информации	+	+	+	ViPNet SIES MC	
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+	+	+	ViPNet SIES MC	
ОДТ.7	Кластеризация информационной (автоматизированной) системы					

XI. Защита ИС/АСУ и ее компонентов

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
ЗИС.0	*Разработка политики защиты информационной (автоматизированной) системы и ее компонентов*	+	+	+		
ЗИС.1	*Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями*	+	+	+		
ЗИС.2	Защита периметра информационной (автоматизированной) системы	+	+	+		
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	+	+	+		
ЗИС.4	Сегментирование информационной (автоматизированной) системы		+	+		
ЗИС.5	Организация демилитаризованной зоны	+	+	+		

XI. Защита ИС/АСУ и ее компонентов

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
ЗИС.6	Управление сетевыми потоками					
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения ("песочница")					
ЗИС.8	**Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы**	+	+	+	ViPNet SIES Core ViPNet SIES Unit	• Обеспечение конфиденциальности информации
ЗИС.9	Создание гетерогенной среды					
ЗИС.10	Использование программного обеспечения, функционирующего в средах различных операционных систем					
ЗИС.11	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом					

XI. Защита ИС/АСУ и ее компонентов

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти					
ЗИС.13	Защита неизменяемых данных		+	+	ViPNet SIES Core ViPNet SIES Unit	• Обеспечение конфиденциальности информации • Обеспечение целостности
ЗИС.14	Использование неперезаписываемых машинных носителей информации					
ЗИС.15	Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек					
ЗИС.16	Защита от спама		+	+		
ЗИС.17	Защита информации от утечек					

XI. Защита ИС/АСУ и ее компонентов

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию					
ЗИС.19	**Защита информации при ее передаче по каналам связи**	+	+	+	ViPNet SIES Core ViPNet SIES Unit	• Обеспечение конфиденциальности информации • Обеспечение целостности
ЗИС.20	Обеспечение доверенных канала, маршрута	+	+	+		
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	+	+	+		
ЗИС.22	Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами					
ЗИС.23	Контроль использования мобильного кода		+	+		

XI. Защита ИС/АСУ и ее компонентов

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
ЗИС.24	Контроль передачи речевой информации		+	+		
ЗИС.25	Контроль передачи видеоинформации		+	+		
ЗИС.27	Обеспечение подлинности сетевых соединений		+	+		
ЗИС.28	Исключение возможности отрицания отправки информации		+	+		
ЗИС.29	Исключение возможности отрицания получения информации		+	+		
ЗИС.31	Защита от скрытых каналов передачи информации			+		
ЗИС.32	**Защита беспроводных соединений**	**+**	**+**	**+**	ViPNet SIES Core ViPNet SIES Unit	• Обеспечение конфиденциальности информации • Обеспечение целостности

XI. Защита ИС/АСУ и ее компонентов

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
ЗИС.33	Исключение доступа через общие ресурсы			+		
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	+	+	+		
ЗИС.35	Управление сетевыми соединениями		+	+		
ЗИС.36	Создание (эмуляция) ложных компонентов информационных (автоматизированных) систем					
ЗИС.37	Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев)					
ЗИС.38	Защита информации при использовании мобильных устройств	+	+	+		

XIII. Управление конфигурацией

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
УКФ.0	*Разработка политики управления конфигурацией информационной (автоматизированной) системы*	+	+	+		
УКФ.1	Идентификация объектов управления конфигурацией					
УКФ.2	Управление изменениями	+	+	+		
УКФ.3	**Установка (инсталляция) только разрешенного к использованию программного обеспечения**	+	+	+	ViPNet SIES Core ViPNet SIES Unit	• Доверенная загрузка файлов конфигурирование • Аутентификация пользователей
УКФ.4	**Контроль действий по внесению изменений**				ViPNet SIES Core ViPNet SIES Unit	• Доверенная загрузка файлов конфигурирование • Аутентификация пользователей

XIV. Управление обновлениями ПО

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Используемый компонент решения	Сценарий работы
		3	2	1		
ПО.0	*Разработка политики управления обновлениями программного обеспечения*	+	+	+		
ОПО.1	**Поиск, получение обновлений программного обеспечения от доверенного источника**	+	+	+	ViPNet SIES Core ViPNet SIES Unit	• Доверенное обновление ПО защищаемого устройства
ОПО.2	**Контроль целостности обновлений программного обеспечения**	+	+	+		
ОПО.3	*Тестирование обновлений программного обеспечения*	+	+	+	ViPNet SIES Core ViPNet SIES Unit	• Доверенное обновление ПО защищаемого устройства
ОПО.4	**Установка обновлений программного обеспечения**	+	+	+	ViPNet SIES Core ViPNet SIES Unit	• Доверенное обновление ПО защищаемого устройства

Сводная таблица

Аутентификация и идентификация	Ограничение программной среды	Обеспечение целостности	Защита ИС/АСУ и ее компонентов	Управление обновлениями ПО
ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.7,	ОПС.1, ОПС.2	ОЦЛ.1, ОЦЛ.2, ОЦЛ.3, ОЦЛ.4, ОЦЛ.5	ЗИС.8, ЗИС.19, ЗИС.32	ОПО.1, ОПО.2, ОПО.4

Управление доступом	Аудит безопасности	Обеспечение доступности	Управление конфигурацией	Компенсирующие меры для:
УПД.1, УПД.2, УПД.3, УПД.4, УПД.13	АУД.4, АУД.6	ОДТ.4, ОДТ.5, ОДТ.6	УКФ.3, УКФ.4	Антивирусная защита: АВЗ.1, АВЗ.3, АВЗ.4, АВЗ.5

СПАСИБО!

Marina.Sorokina@infotecs.ru
Марина Сорокина