DEPO [computers]

Решения
DEPO Security Systems

Security
Systems

Информационная безопасность

Информационная безопасность — это защищенность жизненно важных информационных ресурсов и систем от внешних и внутренних посягательств и угроз для граждан, организаций и государственных органов.

Почему клиент инициирует проект по ИБ?

Забота о реальной информационной безопасности

Необходимость соответствия требованиям законодательства

Решения DEPO Security Systems

Продукт Depo	Описание	ССостав
DEPO Скала-Р		
DEPO vGT		
DEPO Гамаюн		
DEPOКаркас		
DEPO Роса		
DEPO ВКС		
DEPO Terminal		

Основные законы и требования контролирующих органов в области информационной безопасности

Нормативный документ, требования	Объект защиты	Классификация	Контролирующий орган	Область ответственности	Решения DEPO Computers
Федеральный закон 152-ФЗ «О персональных данных»	Персональные данные	4 уровня защищенности	Роскомнадзор	Бумаги	DEPO Cube PD vGT
			ФСТЭК	Техническая защита информации	
			ФСБ	СКЗИ	
Приказ ФСТЭК № 17	Государственные и муниципальные информационные системы	4 класса защищенности	ФСТЭК	Техническая защита информации	
			ФСБ	СКЗИ	
Федеральный закон № 5485-1 «О государственной тайне», требования к ОИ, отнесенных к компетенции ФАПСИ (ФСБ)	Сведения, составляющие государственную тайну	Секретно. Совершенно секретно. Особой важности. ДСП	ФСТЭК	ТЗИ	DEPO Куб ГТ Гамаюн Роса vGT
			ФСБ	ОГВ	
Требования к защите объектов Минобороны России	Сведения, составляющие государственную тайну, на объектах Минобороны России	Секретно. Совершенно секретно. Особой важности.	Минобороны	Объекты Минобороны	DEPO Каркас

Основные законы и требования контролирующих органов в области информационной безопасности

Нормативный документ, требования	Объект защиты	Классификация	Контролирующий орган	Область ответственности	Решения DEPO Computers
Приказ ФСТЭК № 31 (требования к защите АСУ ТП на КВО и ПОО)	Информация в АСУ ТП	3 класса защищенности	ФСТЭК	Техническая защита информации	DEPO Cube PD Depo Security Cloud
			ФСБ	СКЗИ	
Приказ ФСТЭК/ФСБ № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»	Государственные информационные системы общего пользования	2 класса ИСОП	ФСТЭК	Техническая защита информации	
			ФСБ	СКЗИ	

И другие:

- федеральный закон 98-ФЗ «О коммерческой тайне» (контролирующий орган — ФСТЭК);
- стандарт Банка России СТО БР ИББС (контролирующие органы — Банк России, ФСТЭК, ФСБ);
- федеральный закон 161-ФЗ «О национальной платежной системе» (контролирующие органы — Банк России, ФСТЭК, ФСБ).

Деятельность по защите информации (лицензии ФСТЭК)

Наименование	Действие лицензии распространяется на:	Наличие
На деятельность по разработке и производству средств защиты конфиденциальной информации (КИ)	• разработку средств защиты КИ; • производство средств защиты КИ.	Да
На деятельность по технической защите конфиденциальной информации (КИ)	• контроль защищенности КИ от утечки по техническим каналам; • контроль защищенности КИ от несанкционированного доступа и ее модификации КИ в средствах и системах информатизации; • сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты КИ; • аттестационные испытания и аттестацию на соответствие требованиям по защите информации; • проектирование в защищенном исполнении; • установку, монтаж, испытания, ремонт средств защиты информации.	Частично
На осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации)	• контроль защищенности информации, составляющей государственную тайну, аттестацию средств и систем на соответствие требованиям по защите информации; • проведение специсследований на ПЭМИН технических средств обработки информации; • проектирование объектов в защищенном исполнении.	Нет

Деятельность по защите информации (лицензии ФСТЭК)

Наименование	Действия лицензии распространяется на:	Наличие
На осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны	• осуществление мероприятий и (или) оказание услуг в части противодействия иностранным техническим разведкам.	Нет
На проведение работ, связанных с созданием средств защиты информации (ГТ)	• разработку, производство, реализацию, установку, монтаж, наладку, испытания, ремонт, сервисное обслуживание: ○ технических средств защиты информации; ○ защищенных технических средств обработки информации; ○ технических средств контроля эффективности мер защиты информации; ○ программных (программно-технических) средств защиты информации; ○ защищенных программных (программно-технических) средств обработки информации; ○ программных (программно-технических) средств контроля защищенности информации.	Нет

Деятельность по защите информации (лицензии ФСБ)

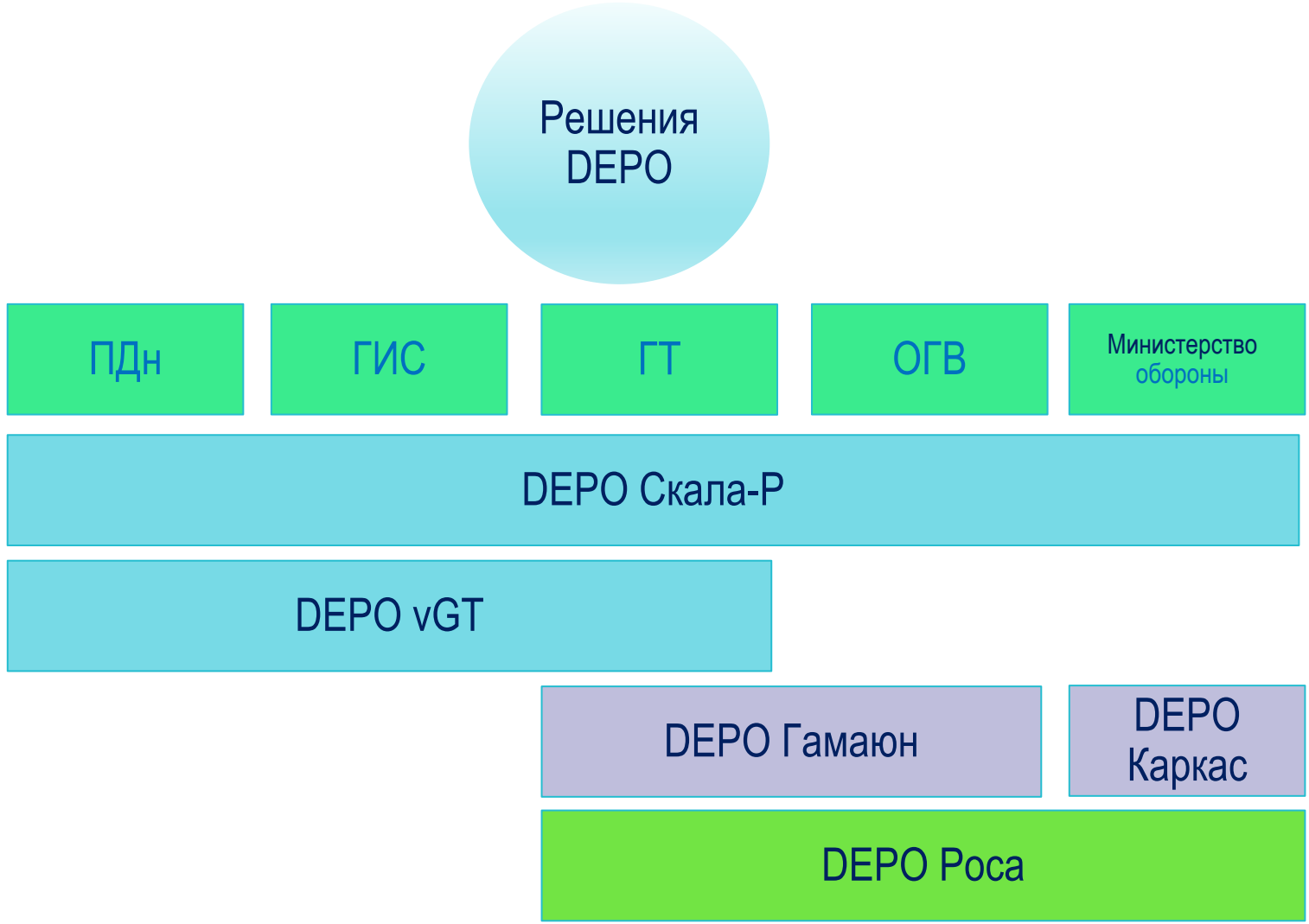
Наименование	Действия лицензии распространяется на:	Наличие
На осуществление работ, связанных с использованием сведений, составляющих государственную тайну	проведение работ, связанных с использованием сведений, составляющих государственную тайну на территории Российской Федерации	Да
Осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны	техническое обслуживание (монтаж, наладка, установка, сервисное обслуживание, ремонт), распространение (продажа, передача): ○ шифровальных средств; ○ защищенных с использованием шифровальных средств информационных систем, систем и комплексов телекоммуникаций; ○ информационных и телекоммуникационных систем органов государственной власти РФ; ○ защищенных средств обработки информации, средств защиты информации (кроме криптографических), предназначенных для использования в органах государственной власти России.	Нет
На осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)		Нет

Деятельность по защите информации (лицензии ФСБ)

Наименование	Действие лицензии распространяется на:	Наличие
Осуществление работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну	• разработку, производство: ○ шифровальных средств; ○ информационных систем, систем и комплексов телекоммуникаций, защищенных с использованием шифровальных средств; ○ информационных и телекоммуникационных систем органов государственной власти РФ; ○ защищенных средств обработки информации, средств защиты информации (кроме криптографических), предназначенных для использования в органах государственной власти России.	Нет
На осуществление разработки и производства средств защиты конфиденциальной информации, предназначенные для использования на объектах Администрации Президента Российской Федерации, Совета Безопасности Российской Федерации, Федерального Собрания Российской Федерации, Правительства Российской Федерации, Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации и Высшего Арбитражного Суда Российской Федерации		Нет
На осуществление выявления электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)	• выполнение работ по выявлению в помещениях электронных устройств, предназначенных для негласного получения информации; • выполнение работ по выявлению в технических средствах электронных устройств, предназначенных для негласного получения информации.	Нет
Осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны	• проведение специальных исследований на побочные электромагнитные излучения и наводки технических средств, предназначенных для использования в органах государственной власти России; • выполнение работ по выявлению в помещениях электронных устройств, предназначенных для негласного получения информации; • выполнение работ по выявлению в технических средствах электронных устройств, предназначенных для негласного получения информации.	Нет

Возможности DEPO Computers по обеспечению ИБ

Решения DEPO Computers
IT Security Compliance Systems



Основные потребители систем ИБ

Федеральный закон 152-ФЗ «О персональных данных»

Персональными данными является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу — субъекту персональных данных.

Федеральный закон от 27.07.06 № 152-ФЗ **«О персональных данных»** вступил в силу 27.01.2007 г. Этим законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой государственными и муниципальными органами, а также юридическими и физическими лицами с использованием или без использования средств автоматизации.

Контролирующими органами выступают Роскомнадзор, ФСТЭК и ФСБ России.

Требования к обработке и защите персональных данных

- Соблюдение условий и принципов обработки персональных данных
- Разработка ряда документов, содержащих описание процессов обработки персональных данных
- Принятие организационных мер, направленных на обеспечение корректной обработки и безопасности персональных данных
- Принятие технических мер защиты персональных данных в соответствии с требованиями законодательства РФ и регулирующих органов
- Осуществление контроля соблюдения требований к обработке и защите персональных данных и эффективности применяемых защитных мер

Риски, связанные с нарушением требований законодательства

- Применение принудительных мер по прекращению или приостановлению обработки персональных данных в связи с нарушением требований действующего законодательства России
- Привлечение компании и ее ответственных лиц к уголовной, административной или иным видам ответственности
- Потеря деловой репутации и конкурентных преимуществ

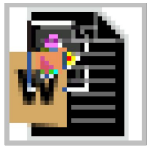
Организации, наиболее часто проверяемые на предмет соблюдения закона о защите персональных данных

- Банки
- Страховые компании
- Коллекторские агентства
- Торговые сети, выдающие карты, по которым предоставляются скидки или бонусы для физических лиц
- Кол-центры, обрабатывающие базы данных физических лиц
- Биржевые брокеры
- Образовательные учреждения
- Медицинские учреждения
- Компании по продаже именных билетов
- Автосалоны и автосервисы
- Туристические агентства
- Кредитные кооперативы
- Гостиницы
- Нотариальные конторы

DEPO PD Cube.
Шаг первый — анкетирование

Для определения основных параметров разрабатываемой системы ИБ необходимо провести анкетирование.

Вопросы представлены в прикрепленном документе.



Опросный лист

DEPO PD Cube.
Шаг второй — определение уровня (класса) защищенности

1. Государственные информационные системы			
Уровень значимости информации	**Федеральный масштаб ГИС**	**Региональный масштаб ГИС**	**Объектовый масштаб ГИС**
1 (нарушение К/Ц/Д* =>высокий ущерб)	К1	К1	К1
2 (нарушение К/Ц/Д => средний ущерб)	К1	К2	К2
3 (нарушение К/Ц/Д =>низкий ущерб)	К2	К3	К3
4 (не возможно определить ущерб)	К3	К3	К4

* К — конфиденциальность, Ц — целостность (неизменность), Д — доступность (безотказность)

DEPO PD Cube.
Шаг второй — определение уровня (класса) защищенности

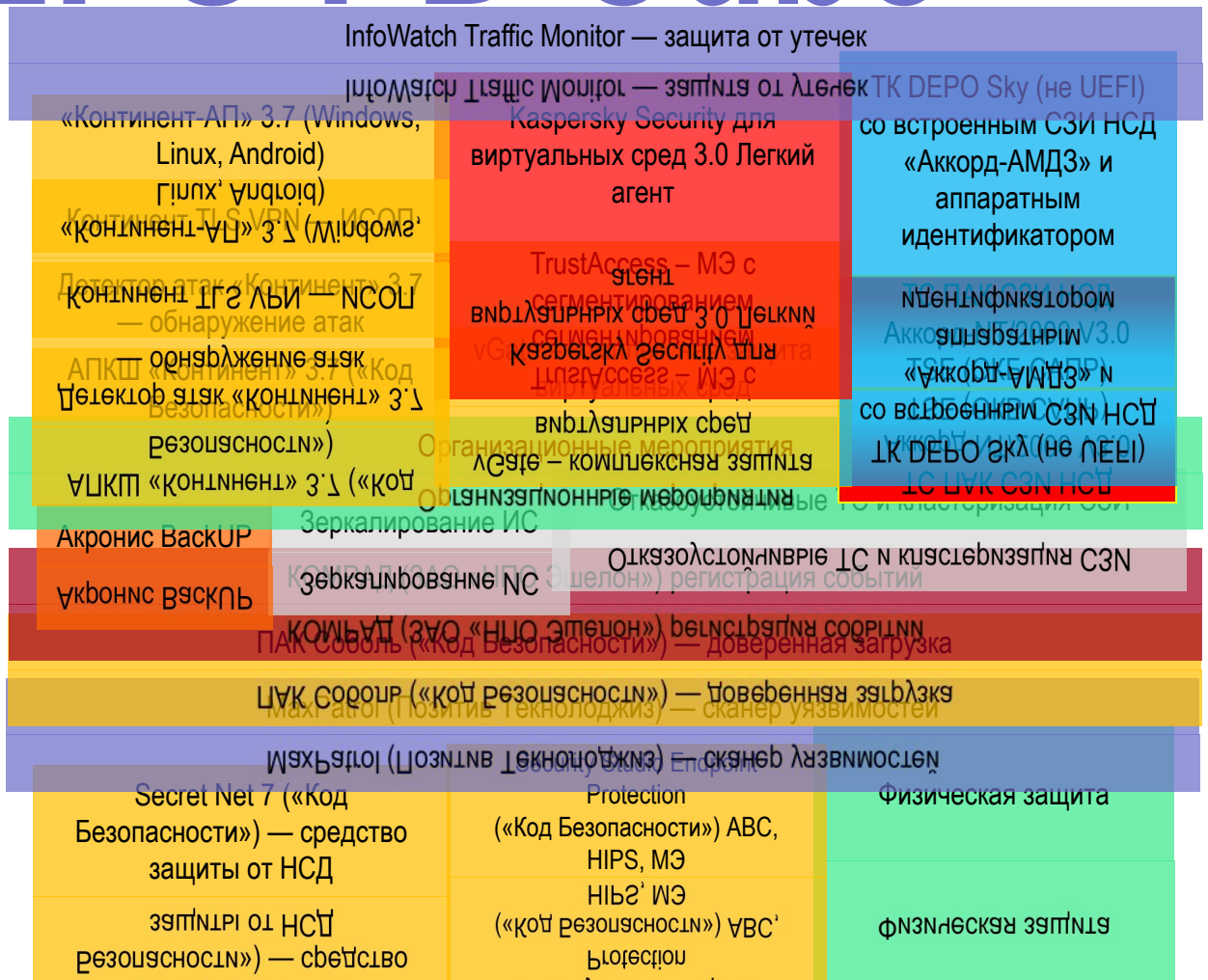
DEPO [computers]

2. Персональные данные

Категории ПДн		Специальные			Биомет-рические	Иные			Общедоступные		
Собственные работники		нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов		> 100 тыс.	< 100 тыс.			> 100 тыс.	< 100 тыс.		> 100 тыс.	< 100 тыс.	
Тип актуальности угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

DEPO PD Cube. Шаг второй — определение уровня (класса) защищенности

DEPO PD Cube



Состав решения Depo PD Cube

ПО Secret Net - средство защиты информации от несанкционированного доступа, состоит из клиентской и серверной части.

ПО Security Studio Endpoint Protection представляет собой сертифицированную систему защиты ПК от сетевых вторжений, спама и вредоносного ПО. Включает межсетевой экран, антивирус, службу обнаружения и предотвращения вторжений.

Программно-аппаратный комплекс ПАК «Соболь» 3.0 – это электронный замок для защиты компьютера от несанкционированного доступа (аппаратно-программный модуль доверенной загрузки). Электронный замок «Соболь» применяется для защиты персональных компьютеров, в том числе десктопов, ноутбуков, ультрабуков, а также серверов и ряда специализированных устройств (криптографических шлюзов, маршрутизаторов и т. д.)

Состав решения Depo PD Cube

Аппаратно-программный комплекс шифрования «Континент» является средством построения виртуальных частных сетей (VPN) на основе глобальных сетей общего пользования, использующих протоколы семейства TCP/IP. АПКШ «Континент» обеспечивает надежную защиту информационных сетей организации от вторжения со стороны сетей передачи данных, конфиденциальных данных при передаче информации по открытым каналам связи (VPN), безопасный доступ удаленных пользователей посредством VPN, защищенное взаимодействие сетей различных организаций, разделение доступа между информационными подсистемами, безопасное взаимодействие со сторонними организациями.

АПКШ «Континент» IP-64 (S088)

АПКШ «Континент» IPC-10 (S088)

АПКШ «Континент» IPC-25 (S115)

АПКШ «Континент» IPC-100 (S102)

АПКШ «Континент» IPC-400 (S021)

«Континент-АП» 3.7 - программный VPN-клиент для ОС Windows, Linux, Android и iOS, применяется для создания защищенного подключения удаленных сотрудников к ресурсам корпоративной сети.

Состав решения Depo PD Cube

«Континент TLS VPN» применяется для создания TLS/SSL VPN-туннеля
Предназначен для решения следующих задач:
Безопасного подключения пользователей к порталам государственных услуг, электронным торговым площадкам, системам интернет-банкинга или корпоративным приложениям через веб-браузер.
Криптографической защиты http-трафика при передаче данных по открытым каналам сетей общего пользования.

Континент TLS VPN Сервер IPC-3000F

Детектор атак «Континент» - аппаратно-программное средство на специализированной аппаратной платформе с предварительно установленными программными модулями детектора атак.

Детектор атак обеспечивает обнаружение основных угроз безопасности информации, относящихся к

Детектор атак «Континент» IPC-1000 (S021)

Состав решения Depo PD Cube

«Континент» уже используют крупнейшие компании и структуры РФ:

- ✔ Министерство Финансов Российской Федерации
- ✔ ГАС «Выборы»
- ✔ Администрация президента России
- ✔ Центральный Банк Российской Федерации (ЦБ РФ)
- ✔ Федеральная Таможенная Служба России (ФТС)
- ✔ Федеральное Казначейство (Казначейство России)
- ✔ Объединенная судостроительная корпорация (ОСК)
- ✔ Министерство обороны Российской Федерации
- ✔ Нефтяные корпорации

Состав решения Depo PD Cube

MAXPATROL
КОМПЛЕКСНЫЙ МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

MaxPatrol позволяет получать объективную оценку состояния защищенности как всей информационной системы, так и отдельных подразделений, узлов и приложений. Механизмы тестирования на проникновение (Pentest), системных проверок (Audit) и контроля соответствия стандартам (Compliance) в сочетании с поддержкой анализа различных операционных систем, СУБД и Web-приложений позволяют MaxPatrol обеспечивать непрерывный технический аудит безопасности на всех уровнях информационной системы.

INFOWATCH® BECAUSE YOUR DATA IS YOUR BUSINESS

ПО InfoWatch Traffic Monitor – современное DLP-решение для защиты данных, предотвращения утечек и контроля перемещения конфиденциальной информации за пределы компании, а также защиты предприятия от внутренних угроз (инсайдеров)

KASPERSKY lab

Kaspersky Security для виртуальных сред Легкий агент — это передовое решение для обеспечения безопасности виртуальных сред, позволяющее сохранить высокий уровень консолидации (плотности ВМ на хост-сервере) и повысить отдачу от вложений в виртуальные серверы и рабочие станции на базе гипервизоров от Microsoft, Citrix или VMware.

Состав решения Depo PD Cube

Средство защиты информации (СЗИ) TrustAccess — распределенный межсетевой экран высокого класса защиты, предназначенный для защиты серверов и рабочих станций локальной сети от несанкционированного доступа, разграничения сетевого доступа к информационным системам предприятия. Внедрение TrustAccess не требует реконфигурирования существующей сетевой инфраструктуры. Продукт пригоден для защиты физических и виртуальных машин, может использоваться как в сетях с доменной организацией, так и в одноранговых сетях.
TrustAccess позволяет управлять доступом к сетевым службам в условиях работы в терминальной среде, разграничить доступ к сетевым ресурсам, например, на основе уровней допуска или должностей пользователей.

TrustAccess состоит из следующих программных компонентов:
• сервер управления TrustAccess — центральная часть, обеспечивающая взаимодействие всех компонентов, обработку и хранение данных. Устанавливается на выделенный сервер (рекомендуется) или на один из компьютеров сети, функционирующий под управлением ОС Windows (например, рабочее место администратора безопасности или защищаемый сервер);
• сервер обработки событий — предназначен для сбора и обработки данных аудита с агентов и с сервера управления;
• сервер построения отчетов — обеспечивает генерацию отчетов на сервере обработки событий;
• агент межсетевого экрана TrustAccess — предназначен для образования доверенного канала передачи данных и обеспечения функции разграничения доступа к защищаемым компьютерам;
• АРМ администратора TrustAccess — обеспечивает централизованное управление средствами и механизмами защиты, абонентами. Устанавливается на рабочее место администратора безопасности.

Состав решения Depo PD Cube

vGate R2 – сертифицированное средство комплексной защиты платформ виртуализации на базе VMware vSphere.

Основные возможности

✔ Выполнение мер по защите среды виртуализации в соответствии с требованиями нормативных актов:

- Приказ ФСТЭК России от 11.02.2013 № 17 – по защите информации в ГИС.
- Приказ ФСТЭК России от 18.02.2013 № 21 – по защите информации в ИСПДн.
- Приказ ФСТЭК России от 14.03.2014 № 31 – по защите информации в АСУ ТП.

✔ Разграничение доступа к управлению виртуальной инфраструктурой

✔ Регистрация и аудит событий безопасности

✔ Защита от специфических угроз, характерных для виртуальных сред:

- Контроль виртуальных устройств.
- Контроль изменений в системе на основе заданных политик безопасности.
- Контроль целостности и доверенная загрузка ESX(i)-серверов и виртуальных машин.

✔ Централизованное управление и контроль

✔ Поддержка распределенных инфраструктур

Состав решения Depo PD Cube для терминальных систем

Защищенные тонкие клиенты ТК Depo Sky со встроенным СЗИ НСД «Аккорд-АМДЗ» - защищенные тонкие клиенты с аппаратно-программным модулем доверенной загрузки и аппаратным идентификатором, - необходимы **в случаях:**

1) ИСПДн, начиная с 3 уровня защищенности с актуальными угрозами 1 или типов.
2) ГИС класса защищенности К3 с наличием подключения к сетям общего пользования.
3) При использовании СКЗИ класса КС2 и выше.

Защищенный терминальный сервер с ПАК СЗИ НСД Аккорд-Win64(TSE) – доверенная загрузка ОС на терминальном сервере и специальное ПО разграничения доступа Аккорд, предназначенное для работы в различных ОС.

«Доверенная загрузка» – это загрузка различных операционных систем только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и аппаратной идентификации / аутентификации пользователя.

Состав решения Depo PD Cube

SIEM система. Предназначена для оперативного оповещения и реагирования на внутренние и внешние угрозы безопасности автоматизированных систем, а также контроля выполнения требований по безопасности информации.

Преимущества

- ✔ **централизованный сбор и анализ данных журналов событий СЗИ, АРМ, серверов и сетевого оборудования;**
- ✔ **удаленный контроль параметров конфигурации и работы автоматизированных рабочих мест;**
- ✔ **оперативное оповещение и реагирование на внутренние и внешние угрозы безопасности автоматизированной системы;**
- ✔ **контроль выполнения заданных требований по безопасности информации, сбор статистики и построение отчетов по защищенности.**

Acronis Backup - программа для резервного копирования и восстановления данных.

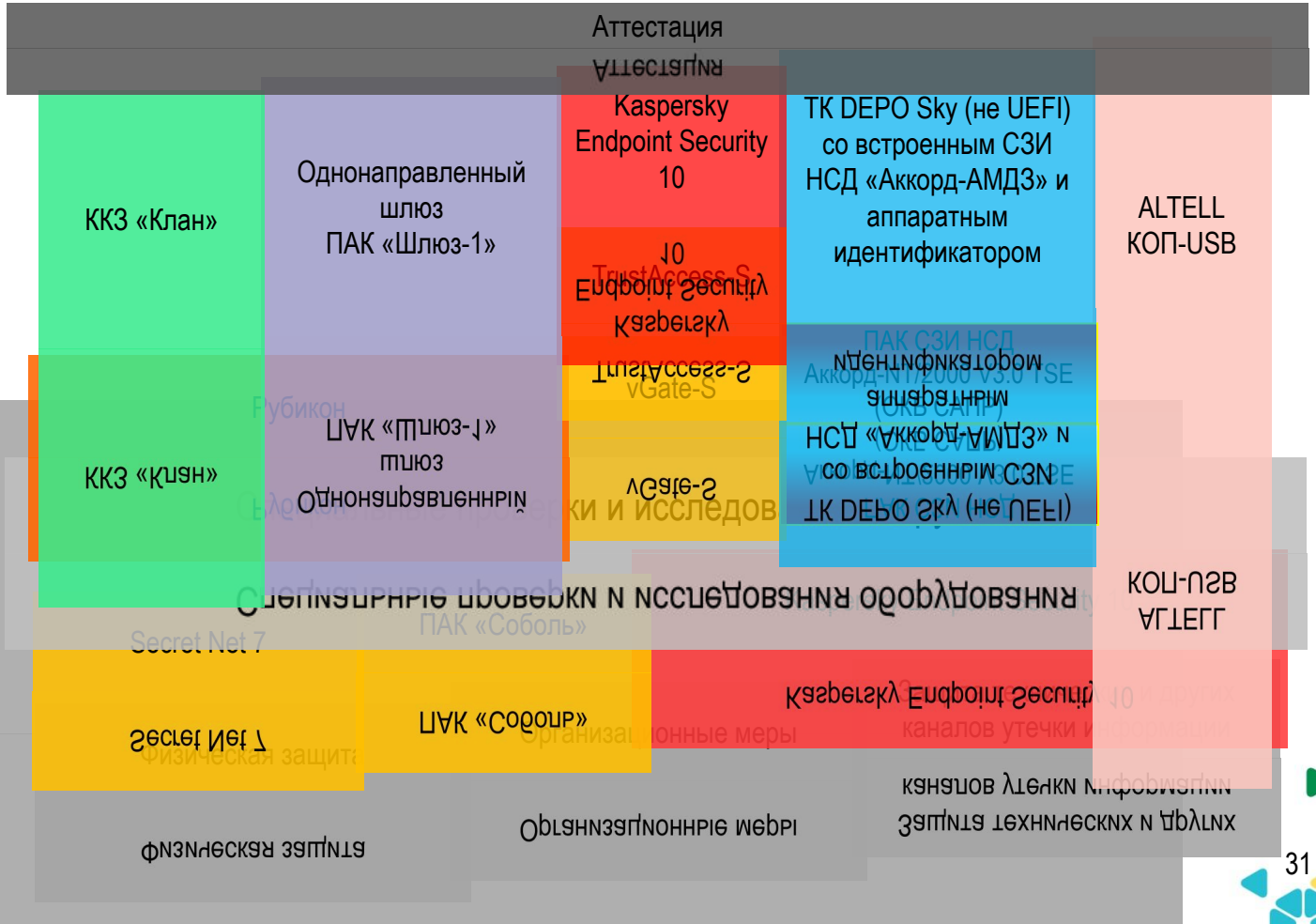
DEPO КУБ ГТ .
Защита государственной тайны

DEPO КУБ ГТ

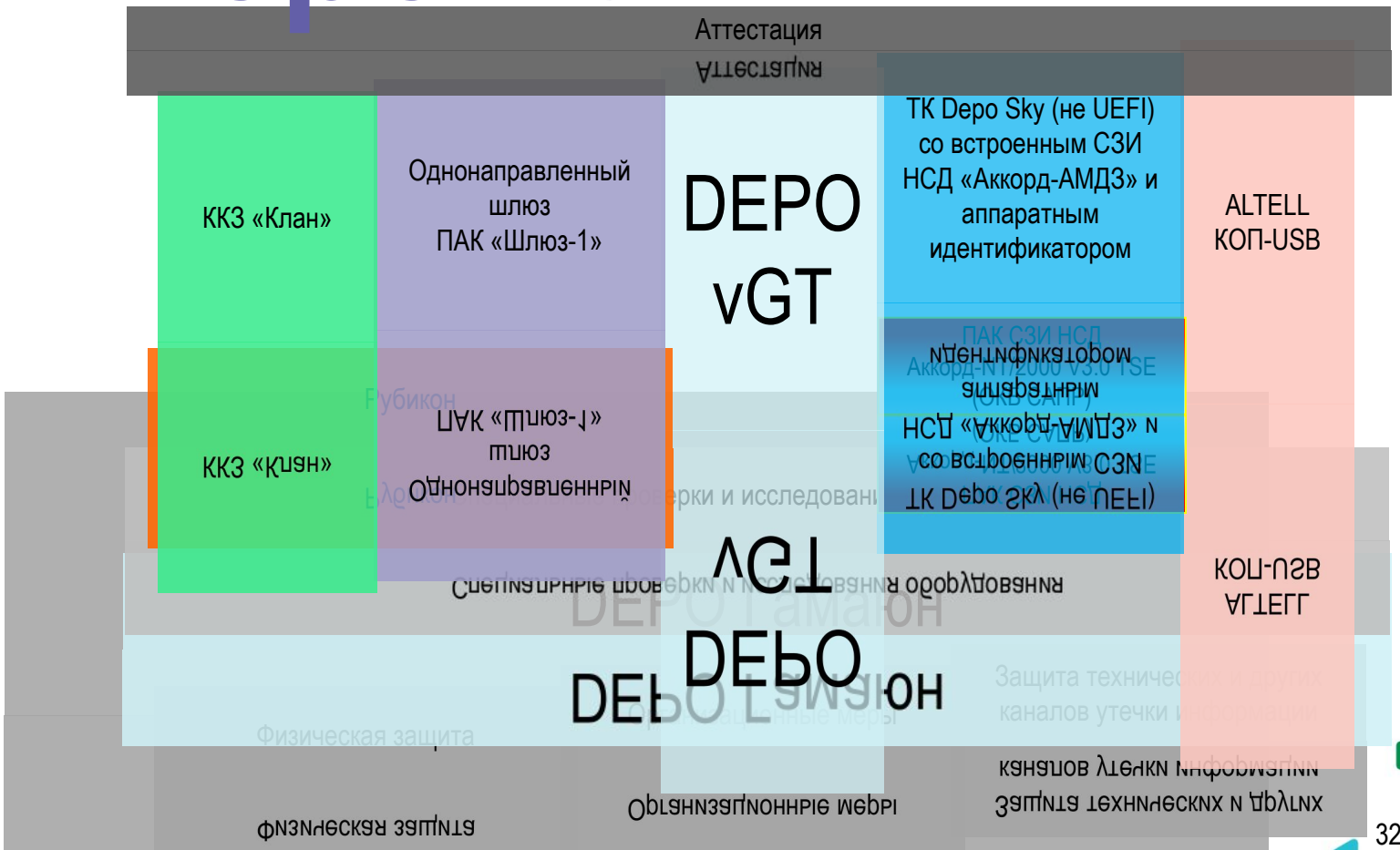
Аттестация

Модуль 2. Передача защищаемой информации по открытым каналам связи (СКЗИ)	Модуль 3. Однонаправленная передача данных между сетями различного уровня секретности	Модуль 4. Обработка защищаемой информации в среде виртуализации (vSec, vAV)	Модуль 5. Обработка защищаемой информации в терминальной среде	Модуль 6. Однонаправленная передача данных через различные интерфейсы

DEPO КУБ ГТ


Аттестация
ККЗ «Клан»
Однонаправленный шлюз ПАК «Шлюз-1»
Kaspersky Endpoint Security 10
ТК DEPO Sky (не UEFI) со встроенным СЗИ НСД «Аккорд-АМДЗ» и аппаратным идентификатором
ALTELL КОП-USB
Secret Net 7
ПАК «Соболь»

Depo КУБ ГТ


Аттестация
ККЗ «Клан»
Однонаправленный шлюз
ПАК «Шлюз-1»
DEPO vGT
ТК Depo Sky (не UEFI) со встроенным СЗИ НСД «Аккорд-АМДЗ» и аппаратным идентификатором
ALTELL КОП-USB
Защита технических и других каналов утечки информации
Физическая защита
Обнаружение вторжений
Защита технических средств

Специальные проверки и исследования

Что это такое?

Специальная проверка (СП) —

это комплекс мероприятий, направленных на поиск и выявление устройств перехвата информации, внедренных в технику.

Специальное исследование (СИ) —

это исследование электромагнитных излучений от оборудования на соответствие нормам при работе с информацией, содержащей государственную тайну.

Что позволит нам их проводить?

Лицензия ФСБ на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны.

Лицензии ФСТЭК на право проведения работ, связанных с созданием средств защиты информации, осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации и (или) противодействия иностранным техническим разведкам).

Лицензия ФСБ на выявление электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах.

Лицензия ФСТЭК на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации).

<u>Для проведения работ в органах государственной власти</u>

Лицензия ФСБ на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (проведение специальных исследований на ПЭМИН технических средств, проведение работ по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах).

Аттестация

Аттестация объектов информатизации — это комплекс организационно-технических мероприятий, в результате которых посредством специального документа — аттестата соответствия — подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России (ФСТЭК России).

Работы по аттестации выполняются в соответствии с «Положением по аттестации объектов информатизации по требованиям безопасности информации» (утверждено Председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994 г.), Национальным стандартом Российской Федерации ограниченного распространения ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения» (принят и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 17.04.2012 г. № 2-ст РО).

Защищаемая информация

Государственная тайна	Конфиденциальная информация

Объект информатизации

Автоматизированные и информационные системы	Выделенные и защищаемые помещения	Системы связи, отображения и размножения информации

Соответствие требованиям нормативно-методических документов

СТР-97 «Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам»	СТР-К «Специальные требования и рекомендации по технической защите конфиденциальной информации»	Приказ ФСТЭК 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

У проводящего аттестацию должно быть

Аттестат аккредитации органа по аттестации	Лицензия на деятельность по технической защите конфиденциальной информации

Основные игроки на рынке СИ по направлению ИБ и производители средств защиты информации

Основные конкуренты

- Информзащита
- Крок
- ИТ-компания «Лета»
- Джет-инфосистем
- РНТ
- Softline

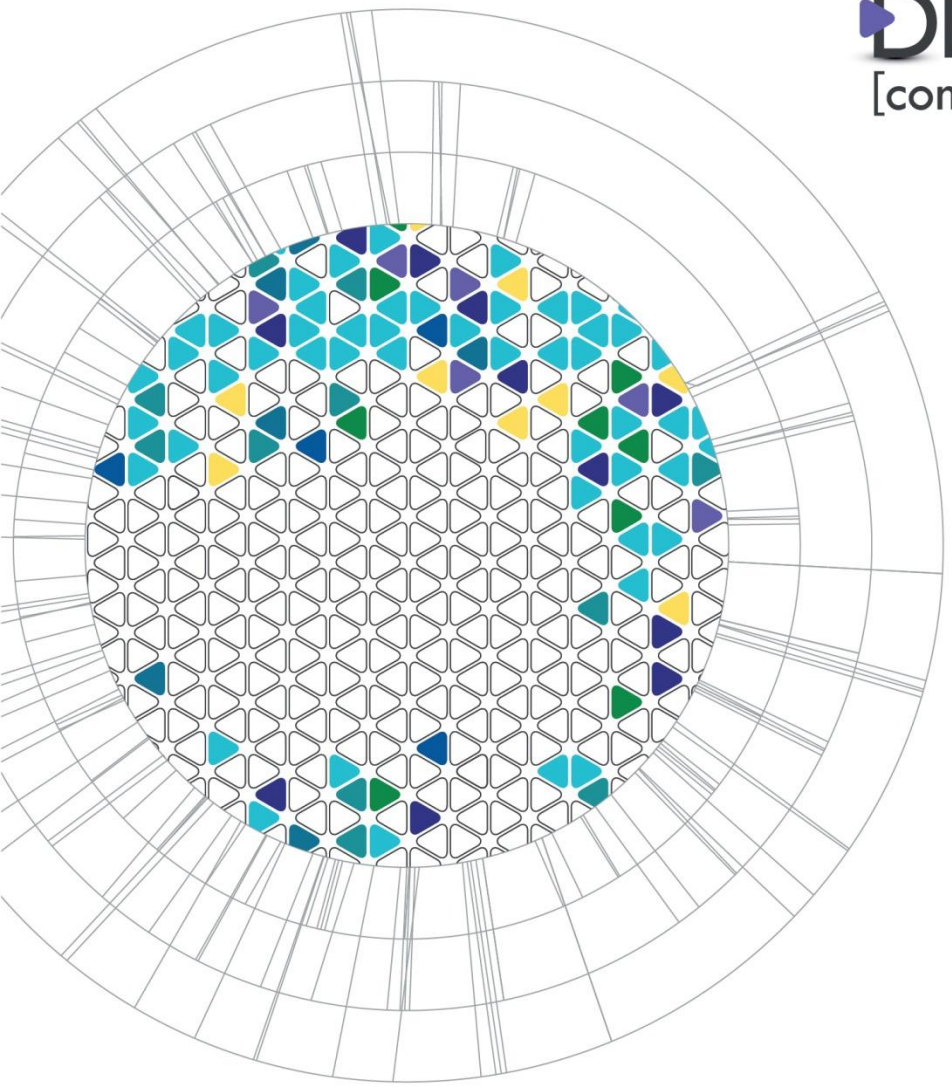
Основные производители

- Код безопасности
- ИнфоТеКС
- ЗАО «НПО Эшелон»
- ОКБ САПР
- ОАО «НПО РусБИТех»
- Kaspersky Lab
- InfoWatch

Список сокращений

Сокращение	Описание
АВС (AV)	Антивирусное средство
АПМДЗ	Аппаратно-программный модуль доверенной загрузки
АСУ ТП	Автоматизированная система управления технологическим процессом
БД	База данных
ГИС	Государственные информационные системы
ГТ	Государственная тайна
ДСП	Для служебного пользования (информация ограниченного доступа)
ИБ	Информационная безопасность
ИСПДн	Информационная система персональных данных
ИСОП	Информационные системы общего пользования (сайты)
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации
СВР	Служба внешней разведки Российской Федерации
СЗИ	Средство защиты информации
СОВ	Средство обнаружения вторжений
УЗ	Уровень защищенности
ФСТЭК	Федеральная служба по техническому и экспортному контролю Российской Федерации
ФСБ	Федеральная служба безопасности Российской Федерации
HIPS	Средство предотвращения вторжений на уровне хоста

DEPO [computers]



Спасибо за внимание!