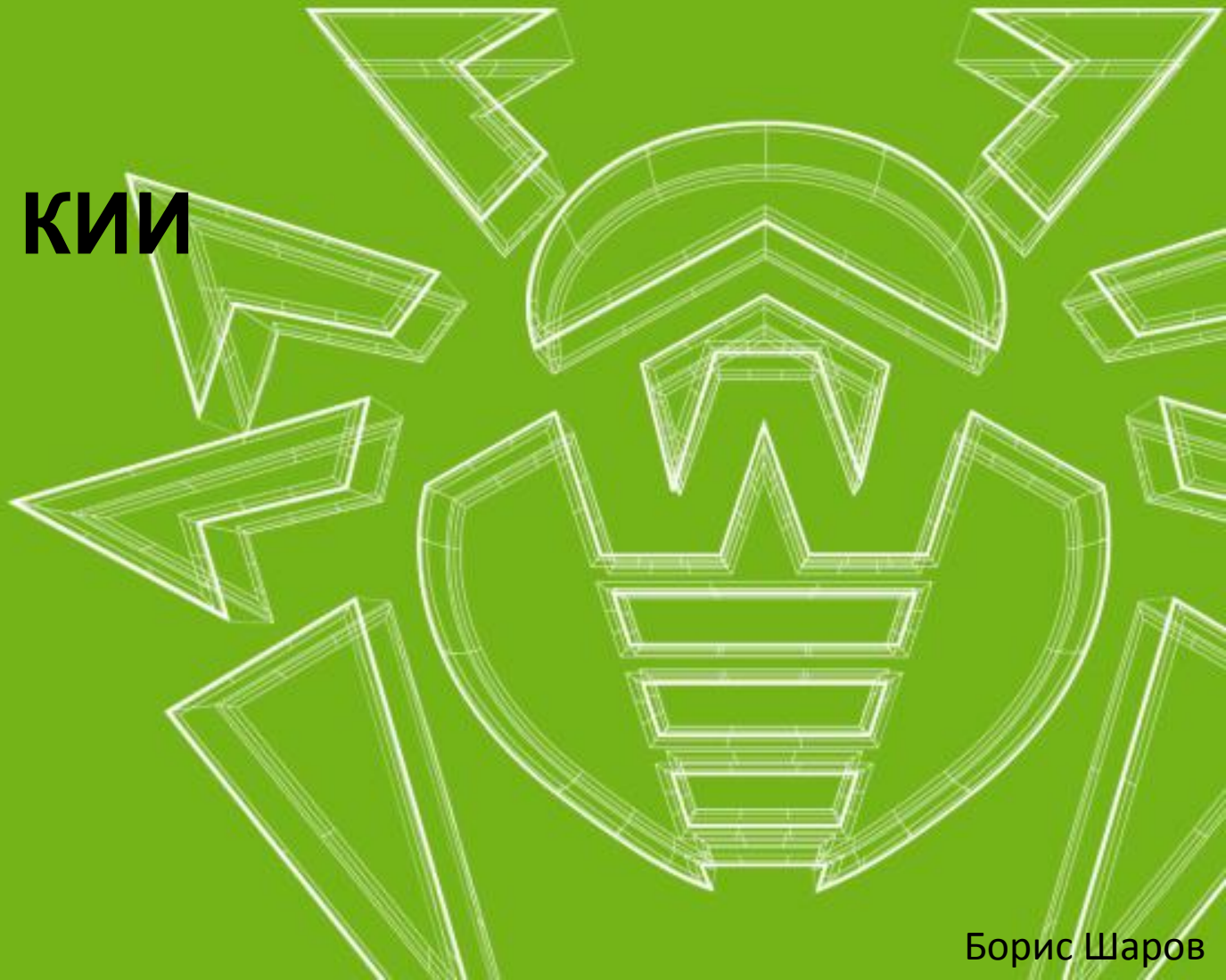
Dr.WEB®
с 1992 года

Совместное решение Dr. Web® и DATAPK® для защиты объектов КИИ

Обзор применимости совместного решения «Доктор Веб» и Cyber Lympha для обеспечения требуемого уровня защиты

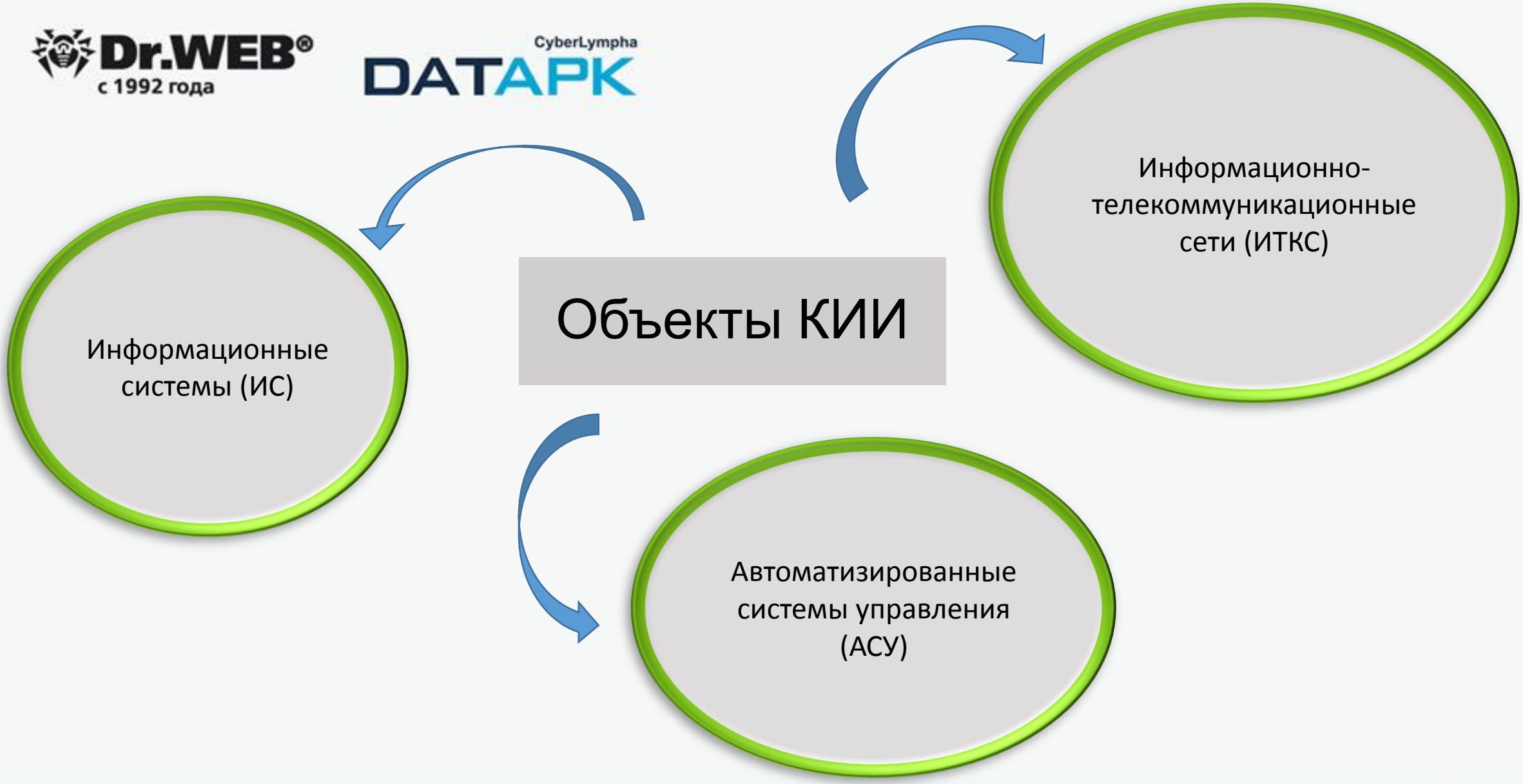


www.антивирус.рф
www.drweb.ru

Борис Шаров

Dr.WEB®
с 1992 года

CyberLympha
DATAPK



Dr.WEB®
с 1992 года

CyberLympha
DATAPK

СЗИ
от несанкционированного
доступа

САВЗ

Межсетевые экраны

Безопасность объектов КИИ

Средства контроля
защищенности

Средства обнаружения
вторжений

Средства управления
событиями
безопасности

Dr.WEB®
с 1992 года

CyberLympha
DATAPK

Антивирусные средства

Защита компонентов объекта КИИ
(наложенные средства)

Средства мониторинга Информационной безопасности

Dr.WEB® с 1992 года

CyberLympha DATAPK

Антивирусные средства (проблематика)

Ложные срабатывания

Чрезмерное потребление ресурсов

Антивирусные средства должны быть специально спроектированы для работы в условиях КИИ

?

Dr.WEB® с 1992 года

CyberLympha DATAPK

Требования к антивирусному средству

- поддержка унаследованных ОС Windows
- поддержка ОС семейства Linux
- контролируемый объем потребляемых ресурсов (чтобы исключить ситуацию с нехваткой вычислительных ресурсов для специального ПО ОКИИ);
- гибкое управление действиями средства антивирусной защиты (в частности, запрет на автоматическое блокирование потенциально вредоносного ПО или удаление файлов), что снижает потенциальный ущерб от ложных срабатываний;
- реализация дополнительных функций узловой защиты: контроль съемных носителей, ведение «белого» списка процессов, межсетевой экран уровня узла (что минимизирует количество средств защиты, которые нужно устанавливать непосредственно на СВТ ОКИИ).

Dr.WEB® с 1992 года

CyberLympha DATAPK

Dr. Web Enterprise Security Suite

- удовлетворяет всем перечисленным требованиям,
- обладает гибкими инструментами централизованного управления,
- имеет продолжительный опыт эксплуатации на критичных системах,
- относящихся к государственным информационным системам (с 2004 года)

Dr.WEB®
с 1992 года

CyberLympha
DATAPK

Dr. Web® Enterprise Security Suite

Разработанная компанией «Доктор Веб» система централизованной антивирусной защиты предприятия любого масштаба и распределенности – **Dr.Web Enterprise Security Suite** – мультиплатформенное решение, дающее возможность надежно защитить любые узлы корпоративного сегмента, независимо от места их нахождения.

Dr.WEB®
с 1992 года

CyberLympha
DATAPK

Защита важнейших государственных объектов

Dr.Web Enterprise Security Suite была разработана для обеспечения антивирусной защиты ГАС «Выборы» Центральной избирательной комиссии Российской Федерации и вступила в строй в 2004 году.
Более 4000 избирательных участков по всей территории страны были защищены антивирусом Dr.Web, который обновлялся с центрального сервера в Москве.

Dr.WEB®
с 1992 года

CyberLympha
DATAPK

Основной функционал Dr.Web Enterprise Security Suite, использованный в защите компьютерной сети ГАС «Выборы»

- стабильность работы, устойчивость к любым сбоям других компонентов системы
- возможность обновлений антивирусных баз по самым слабым каналам связи
- минимальный сетевой трафик при обновлениях
- мониторинг состояния безопасности всех узлов антивирусной сети с единого сервера в ЦИК

Dr.WEB®
с 1992 года

CyberLympha
DATAPK

Развитый функционал, опыт эксплуатации Dr. Web ESS в составе критичных информационных систем,
а также широчайший перечень поддерживаемых ОС делает его одним из наиболее оптимальных средств антивирусной защиты для объектов КИИ.

Dr.WEB®
с 1992 года

CyberLympha
DATAPK

Одним из основных требований, предъявляемых к средствам антивирусной защиты в системах АСУ ТП, является минимальное воздействие на технологические процессы, а также возможность ограничивать потребление системных ресурсов.

Проведенные коллегами из Cyber Lympha тесты 12-й версии Dr.Web® Enterprise Suite показали, что Dr.Web® Enterprise Security Suite полностью отвечает этим требованиям.

Dr.WEB®
с 1992 года

CyberLympha
DATAPK

Компании «Доктор Веб» и компания Cyber Lympha предлагают совместное решение, позволяющее выполнить все требования 239 Приказа ФСТЭК и надежно защищающее практически любого объекта КИИ

Это решение основано на совместном использовании Dr.Web® Enterprise Security Suite и программно-аппаратного комплекса оперативного мониторинга и контроля защищенности АСУ ТП DATAPK®.

Dr.WEB®
с 1992 года

CyberLympha
DATAPK

DATAPK® - универсальное средство мониторинга ИБ, обладающее достаточной гибкостью, чтобы функционировать в среде любого ОКИИ без необходимости доработки со стороны производителя.

DATAPK® реализует:

- идентификацию объектов защиты ОКИИ и информационных связей между ними
- управление конфигурацией объектов защиты
- управление событиями ИБ
- выявление сетевых аномалий
- поиск известных уязвимостей и контроль соответствия требованиям в области ИБ

Dr.WEB® с 1992 года

CyberLympha DATAPK

Dr.Web® Enterprise Security Suite	DATAPK®
Обеспечивает комплексную защиту узлов ОКИИ от угроз ИБ, прежде всего, от внедрения вредоносного кода	Выявляет несанкционированные изменения конфигурации встроенных механизмов ИБ СВТ, что исключает деградацию системы защиты со временем.
Осуществляет мониторинг состояния безопасности узлов сети и передает в Центр управления информацию о состоянии защищенности каждого узла, в том числе, об обновлениях антивирусных баз, а также событиях ИБ, связанных с возможными попытками проникновения ВПО	Обеспечивает единую точку сбора и анализа событий ИБ (от общесистемного и прикладного ПО СВТ ОКИИ, сетевого оборудования, сервера управления Dr. Web и пр.), что позволяет получить общую картину состояния защищенности объекта

Dr.WEB®
с 1992 года

CyberLympha
DATAPK

Дальнейшее развитие совместного решения Dr.Web Enterprise Security Suite + DATAPK

тестирований совместимости совместного решения Dr. Web ESS и DATAPK с производителями решений, используемых в составе ОКИИ (в стадии завершения)*

усиление степени интеграции решений, в том числе, для реализации элементов автоматического реагирования на выявленные инциденты ИБ

* Протоколы совместного тестирования могут быть представлены по запросу.

Dr.WEB®
с 1992 года

CyberLympha
DATAPK

Вопросы?

Благодарим за внимание!