Компания «Доктор Веб»

Российский производитель
антивирусных средств защиты
информации под маркой Dr.Web

Dr.WEB®
с 1992 года

Защити созданное

АНТИВИРУСНАЯ ЗАЩИТА

АСУ ТП объектов ТЭК

МИНИМИЗАЦИЯ РИСКОВ

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

АСУ ТП объектов ТЭК – это закрытый комплекс, поэтому говорить о том, что вредоносные программы могут легко проникнуть в него – неверно.

Несмотря на закрытость, а так же на то, что в информационных системах ТЭК (на рабочих станциях, серверах и т.д.) установлен антивирус и иные средства обеспечения безопасности (например, разграничение прав доступа к различным системам), **в этих защищенных по всем требованиям сетях могут присутствовать вредоносные программы.**

С чем это связано?

Обеспечивает ли антивирус реальную защиту от вирусов?

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Для того, чтобы обезопасить ключевые элементы информационной инфраструктуры – необходимо защитить «периметр», т.е. узкие места в системе предприятия, через которые может проникнуть вредоносное ПО.

Некоторые ошибочно считают, что если подсистема полностью находится в **изолированной зоне** и удаленный доступ к ней невозможен, то ей ничего не угрожает.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Каким образом в периметр объекта ТЭК могут попасть вредоносные программы?

Через уязвимости и слабые места в организации безопасности информационных систем предприятий.

Поэтому очень важно определить возможные уязвимости, через которые может проникнуть угроза.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Какие это могут быть слабые места?

Это могут быть узлы для контроля и управления производственными процессами, напрямую подключенные к интернету и работающие со стандартными настройками, включая пароли.

Вредоносные программы могут попасть в систему посредством устройств и каналов связи, операционных систем и приложений, у которых есть связь между офисом и производством.

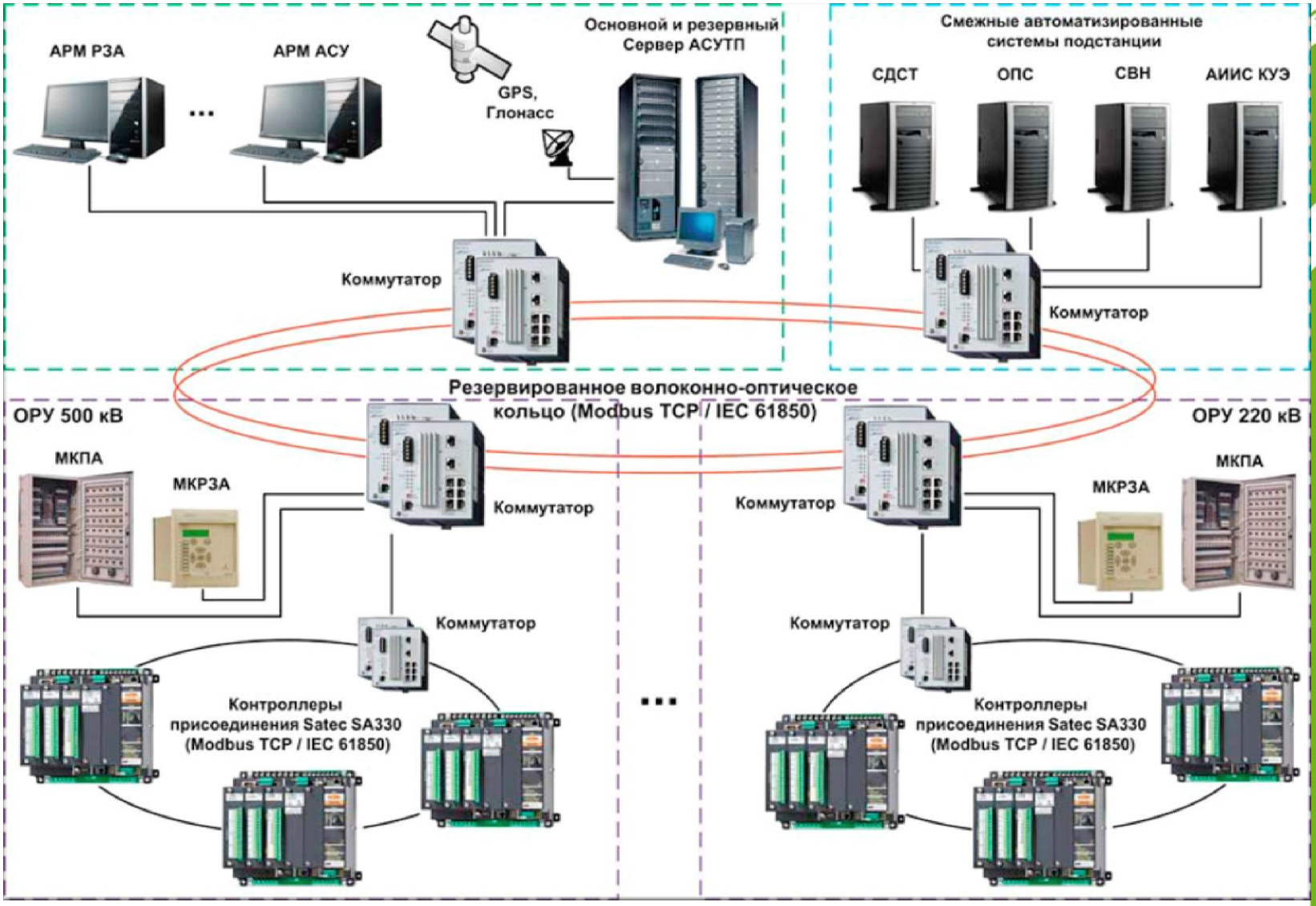
Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Пример структурной схемы АСУ ТП подстанции



(источник: http://www.en-pro.ru/)

Защити созданное

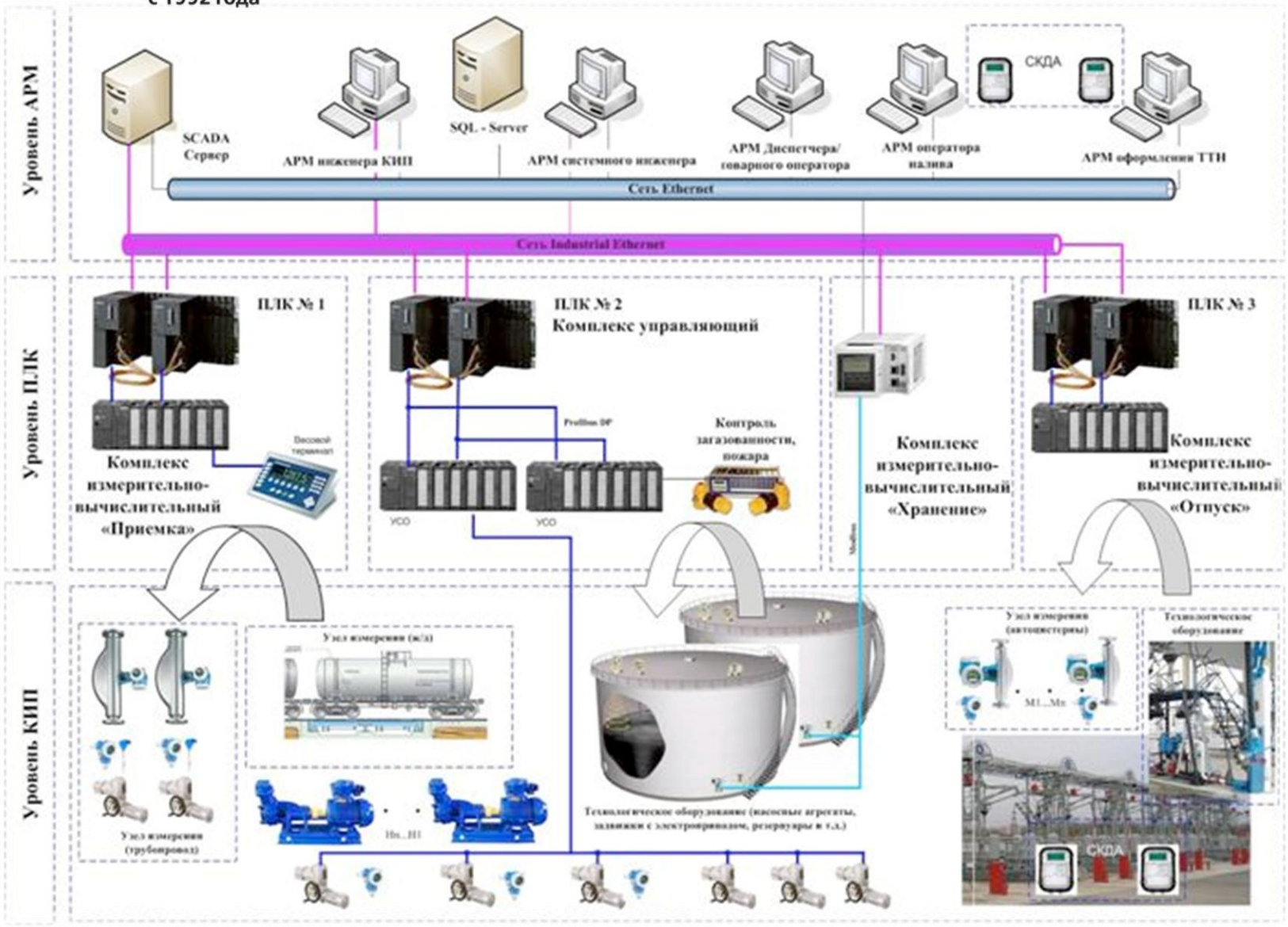
Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Пример структурной схемы АСУ ТП нефтебазы



(источник: http://www.mcee.ru/)

Защити созданное

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Угрозы могут возникнуть изнутри самого объекта ТЭК, т.е. от людей, которые работают на данном объекте, **или инсайдеров**. Очень существенную роль в возникновении вирусных инцидентов играет **человеческий фактор.**

Сотрудниками компании могут двигать как **осознаваемые мотивы причинения вреда объекту** (денежная мотивация от конкурирующей компании, недовольство карьерой или напряженные отношения с коллегами и т.д). По этим причинам в ряде случаев сотрудник может ввести в систему вредоносные программы или похитить важную информацию.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Причины могут быть и неосознанные: игнорирование рекомендаций по выполнению действий, предписанных для повышения информационной безопасности на объекте ТЭК и непонимание возникающих в связи с этим возможных угроз и их последствий.

Безусловно, все сотрудники объектов ТЭК проинструктированы, подписывали документы о неразглашении, технику безопасности и т.д. Но всегда ли соблюдаются эти правила?

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Наряду с тем, что сотрудников необходимо инструктировать и донести до них важность соблюдения правил техники информационной безопасности при нахождении на объекте ТЭК, необходимо также применять средства антивирусной защиты на АРМах, серверах, почтовых шлюзах, средствах межсетевого экранирования, прокси-серверах, мобильных технических средствах и прочих устройствах, которые, располагаются «вокруг» критически важных объектов и могут быть подвержены заражению вредоносными программами, **что может повлиять на работу операционных систем реального времени (ОСРВ).**

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Нет смысла говорить о безусловной важности защиты компьютеров, которые имеют доступ к ОСРВ. Защита связанных с ними управляющих АРМов крайне важна для того, чтобы исключить возможность ошибки в выдаче команды для исполнительного устройства, что может нарушить цикличность процесса, и повлечет за собой серьезные последствия.

Необходимо проведение периодических проверок устройств при старте системы или в период ее обслуживания. Необходимы **и повторные проверки**, в связи с тем, что на момент проникновения вредоносная программа может быть неизвестна антивирусной системе – но станет известной после очередного обновления.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

В нашу антивирусную лабораторию ежедневно поступает порядка 250 тысяч неизвестных экземпляров файлов, требующих проверки. Поэтому важно не только не пустить вирус в систему на «входе», но и обезвредить те вредоносные программы, которые все же обошли АВ и уже присутствуют в системе.

Для того, чтобы вирус дольше оставался неизвестным, злоумышленники сначала проверяют его на всех имеющихся антивирусах. В связи с этим в момент проникновения средства антивирусной защиты не могут предотвратить попытку заражения.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Проблематична и зачастую невозможна установка антивирусных средств на устройства с малым размером оперативной памяти (старые компьютеры, сетевые устройства, принтеры). При этом заражение данных устройств или использование их злоумышленниками возможно, но для установки и работы современных средств защиты не хватает ресурсов.

Что следует предпринять в таких случаях?

В подобных ситуациях защита от вредоносных программ осуществляется путем изоляции данных систем и проведением периодической антивирусной проверки, если это возможно. Это позволит уменьшить риск возникновения вирусных инцидентов.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Вот еще пример возможной уязвимости: Защита серверов средствами антивирусной защиты может не подразумевать защиту сервисов, работающих на них. Так установка постоянной антивирусной защиты сервера (файлового монитора), не будет означать проверки почты проходящей через Операционную Систему MS Exchange.

В связи с этим на серверы нужно устанавливать несколько средств антивирусной защиты.

Защита серверов должна включать проверку файлов, получаемых из внешних источников работающими сервисами (в том числе сервисами электронной почты) в масштабе времени, близком к реальному.

В случае невозможности установки средств постоянной антивирусной защиты, необходимо обеспечить изоляцию устройства от сети интернет, а также сегментов информационной сети.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Использование антивирусных средств защиты обязательно должно дополняться выносом критически важных систем в отдельные сегменты, а критически важных сервисов на отдельные компьютеры.

Также должна использоваться система периодического создания резервных копий.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Крайне важно наличие в антивирусной системе Центра управления – в первую очередь, для невозможности отключения обновлений и компонентов защиты системы.

Для усиления антивирусной защиты АСУ ТП на объектах ТЭК, мы также рекомендуем:

Не наделять администраторов безопасности предоставлением повышенных прав в централизованной системе управления антивирусной защитой, а обеспечить разграничение прав между несколькими администраторами безопасности.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

В информационной системе должна обеспечиваться регистрация событий о неуспешном обновлении антивирусных баз данных.

Важно, чтобы антивирусная система обладала системой самозащиты, контролирующей все попытки обращения к своим компонентам, в том числе с целью изменения настроек или завершения работы антивирусной защиты. Таким образом, установленное Антивирусное ПО продержится до поступления обновлений, в которые уже будет включена информация по новым появившимся вирусам.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Не следует думать, что зараженные файлы станет видно сразу и их обнаружение будет легкой задачей.

Угроза может прийти в виде комплекса из разных файлов – в разное время, по разным каналам. Эти файлы в отдельности не будут вредоносными и на них могут не обратить пристального внимания.

Целенаправленная атака обнаруживается не сразу после попадания в сеть или на атакуемое устройство, а спустя дни, недели или даже месяцы. Угроза может долгое время незаметно находиться в сети и собирать информацию, передавая ее за пределы защищаемого периметра.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Обеспечит ли все вышеперечисленное гарантированную защиту от вредоносных файлов?

От всех возможных вирусных инцидентов – вряд ли.

Но для атак на компьютерные системы предприятий кибермошенники успешно эксплуатируют:

- недостатки построения антивирусных систем защиты различных узлов корпоративной сети,
- недостатки или полное отсутствие на предприятиях политики ИБ,
- несоблюдение сотрудниками предприятий политик ИБ по причинам неграмотности и халатности.

Поэтому, нередко для проникновения, злоумышленникам не обязательно именно «взламывать» систему – достаточно обнаружить узкие места и использовать их.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Службам безопасности объектов ТЭК необходимо постоянно перепроверять собственную политику информационной безопасности

Технологии не стоят на месте, и может оказаться так, что те способы защиты, которые успешно применялись несколько лет назад – на данном этапе времени окажутся устаревшими. Необходимо постоянно проверять систему на наличие «узких мест» в периметре, откуда возможна утечка информации. На основе полученных данных следует дорабатывать и усиливать защиту.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Люди, считающие, что у них идеальный антивирус и идеально выстроенная система защиты, не имеющая слабых мест – скорее всего имеют зараженный компьютерный парк. Просто пока еще не догадываются об этом.

Хороший администратор безопасности – это человек, постоянно сомневающийся в том, что информационные системы его объекта достаточно защищены.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Так как расследование вирусозависимых компьютерных инцидентов не может быть обеспечено администраторами, Вы можете обратиться в нашу компанию для проведения данной экспертизы. Все исследования производятся с соблюдением требований действующего законодательства РФ.

Компания «Доктор Веб» является российским разработчиком средств защиты информации. Продукты Dr. Web разрабатываются с 1992 года и обеспечивают надежную антивирусную защиту крупнейших государственных и коммерческих организаций. Также у нас есть продукты для домашних пользователей.

Продукты Dr Web имеют сертификаты соответствия ФСТЭК, ФСБ и Минобороны России. Это позволяет использовать их в организациях с повышенными требованиями к уровню безопасности, в том числе и на объектах ТЭК.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

В заключение:

Система обеспечения информационной безопасности любого предприятия, в частности реализация мер по антивирусной защите АСУ ТП объектов ТЭК, будет максимально эффективной, если будет соблюдаться комплексная защита всего периметра предприятия.

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

Dr.WEB®
с 1992 года

Защити созданное

Спасибо за внимание!

Москва, 3-я улица Ямского поля, вл. 2 корп. 12А

Тел.: +7 (495) 789-45-87
Факс: +7 (495) 789-45-97

www.drweb.com

ООО «Доктор Веб»

Москва, 3-я улица Ямского поля,
вл. 2 корп. 12А
Тел.: (495) 789-45-87
Факс: (495) 789-45-97
www.drweb.com