Positive Technologies
MultiScanner

ОПИСАНИЕ ПРОДУКТА

POSITIVE TECHNOLOGIES

Согласно исследованию M-Trends Report, в 2014 году 100% жертв крупных взломов и утечек имели у себя своевременно обновляемый антивирус, но это им не помогло.

1. МНОГОУРОВНЕВАЯ ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО: КЛЮЧЕВЫЕ ЗАДАЧИ

Количество и разнообразие вредоносных программ неуклонно растет. Зараженные файлы, письма и веб-сайты все чаще наносят ущерб бизнесу, госструктурам и частным лицам, несмотря на активное использование антивирусных программ. Причина в том, что антивирусные компании не успевают поддерживать актуальными свои базы знаний и не могут обеспечить стопроцентную защиту от всех новых угроз. Кроме того, существует множество продвинутых атак, направленных на обход установленных антивирусов. Все это вынуждает крупные компании использовать облачные сервисы кросс-проверок для повышения уровня обнаружения зловредов, что в свою очередь повышает вероятность утечки конфиденциальной информации.

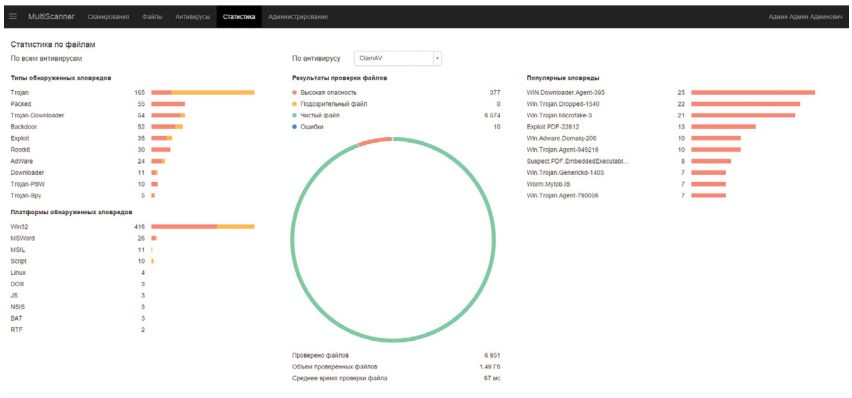
Лучшее решение этих проблем — использование локальной (установленной внутри защищаемого периметра) системы контроля файлов, с возможностью автоматизированной параллельной проверки файлов на нескольких антивирусных решениях и с использованием репутационных сервисов. Для этих задач была создана система выявления вредоносного контента PT MultiScanner.

Это решение Positive Technologies позволяет значительно повысить точность и оперативность обнаружения угроз за счет параллельного сканирования несколькими антивирусными ядрами в сочетании с другими методами выявления вредоносных активностей — включая ретроспективный анализ и репутационные сервисы.

2. PT MULTISCANNER: КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

PT MultiScanner не только противодействует отдельным зловредам, но и помогает выявлять многоступенчатые атаки (APT) и расследовать инциденты — за счет интеграции широкого набора аналитических инструментов:

+ **Сила десятков антивирусов** позволяет как можно быстрее обнаруживать появление новых зловредов. Файлы параллельно сканируются несколькими антивирусами, набор которых пользователи могут формировать самостоятельно.



+ **Обновление антивирусов без доступа к интернету** позволяет работать в изолированных сегментах сети и пресекать возможные утечки данных.

+ **Ретроспективный анализ** дает возможность выяснить, какие системы подвергались воздействию зловредного ПО в прошлом — до того, как оно стало известно антивирусам. PT MultiScanner перепроверяет ранее проверенные файлы при изменении антивирусных баз, и таким образом обнаруживаются ранее пропущенные зловреды.

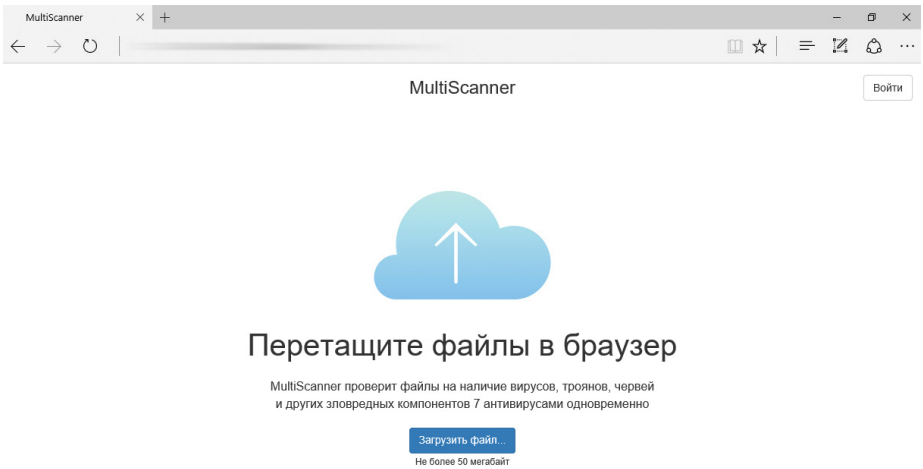
- **Единая внутренняя база знаний и репутационные списки** постоянно обновляются — и выявляют то, что пропустили антивирусы.
- **Поддержка стандартных интерфейсов** (RestAPI, SMTP, ICAP, syslog), возможность мониторинга файловых ресурсов и сетевого трафика позволяют легко встраивать систему в инфраструктуру заказчика.

3. PT MULTISCANNER: СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

PT MultiScanner поддерживает различные сценарии развертывания и применения. Он может использоваться не только для выборочной проверки файлов, но и для защиты веб-приложений и порталов, почтового трафика, файловых хранилищ, архивов — в реальном времени.

3.1. Пользовательский сервис для проверки файлов

Для выборочной проверки PT MultiScanner может применяться в качестве локального пользовательского сервиса. Он устанавливается внутри контролируемого периметра организации. Через веб-интерфейс в PT MultiScanner загружаются отдельные файлы для их проверки на наличие вредоносного содержимого. Доступ к веб-интерфейсу предоставляется как авторизованным, так и анонимным пользователям. Поддерживается несколько схем авторизации (внутренняя по логину и паролю, внешняя (OAuth)). Кроме того, файлы можно проверить отправив их на специально настраиваемый почтовый адрес PT MultiScanner. Также можно просматривать результаты проверок и общую статистику работы системы, подбирать антивирусное решение из списка для каждой задачи сканирования.

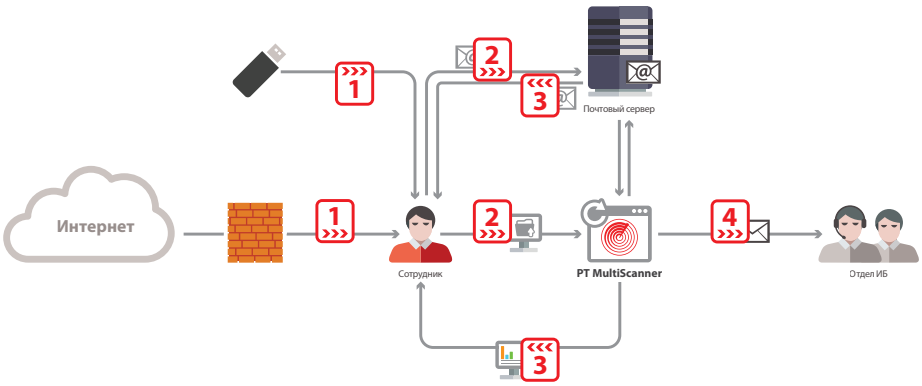


PT MultiScanner позволяет:

- анализировать загружаемые вручную отдельные файлы, письма;
- вести базу знаний по загруженным объектам и вердиктам;
- получать статистику по загруженным файлам и результатам проверок антивирусными средствами;
- проводить ретроспективный анализ;
- уведомлять пользователей об обнаруженном вредоносном содержимом в ранее загруженных файлах;
- отправлять файлы на проверку по почте;
- выдавать результаты в веб-консоли или по электронной почте;
- делиться результатами проверки даже с пользователями, не имеющими учетных записей в сервисе (создавая специальную ссылку).

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

- **Адаптируемость к политике безопасности компании.** В состав PT MultiScanner можно включить те антивирусы, которые соответствуют требованиям ИБ. Кроме того, есть возможность наращивать как число антивирусов, так и пропускную способность системы — для решения конкретных задач заказчика.
- **Работа с архивами.** PT MultiScanner распаковывает архивы и сканирует файлы по отдельности. Это удобно: можно отправить архив и получить вердикты по каждому файлу внутри. Если архив отправлен по почте частями, то PT MultiScanner соберет их в один том, распакует и проверит. Кроме того, PT MultiScanner распаковывает архивы, защищенные паролем. В этом случае система ищет информацию о пароле в теле письма или подбирает его по набору стандартных паролей.
- **Конфиденциальность.** Проверяемые файлы не покидают инфраструктуры системы.
- **Экспертный инструмент для точечного глубокого анализа.** PT MultiScanner дает заказчикам возможность вручную проводить детальный анализ поведения веб-браузеров при переходе по подозрительным веб-ссылкам, а также наблюдать за поведением отдельных исполняемых файлов или установленных легитимных приложений при открытии в них специфических документов — посредством интеграции с исследовательской средой Positive Technologies. Запуск приложений и анализ их поведения происходит в изолированной среде, гарантирующей нераспространение вредоносного содержимого при проверке его в системе. Скрытая от детектирования среда исполнения позволяет долгое время незаметно наблюдать за вредоносным ПО. Можно создавать свои ловушки с заданным ПО и пользовательским окружением, используемым в компании.



Организация выделенного локального сервиса

Пример сценария использования:

1. Пользователь скачивает из сети или загружает с внешнего носителя файл для проверки.
2. Пользователь отправляет этот файл на проверку в PT MultiScanner через веб-портал или через специально настраиваемый почтовый адрес.
3. PT MultiScanner выполняет статический анализ и анализ по репутационным сервисам, по итогам пользователь получает результаты сканирования непосредственно в веб-интерфейсе или по почте.
4. В случае если вредоносное содержимое в файле было найдено при первичном сканировании или при ретроспективном анализе после обновления антивирусных баз или репутационных сервисов, PT MultiScanner отправляет автоматическое уведомление об инциденте отделу ИБ.

3.2. Контроль трафика

PT MultiScanner может использоваться для анализа открытого трафика (например, почтового или пользовательского веб-трафика). Такой анализ может быть проведен в пассивном или активном режимах защиты — в зависимости от потребностей организации.

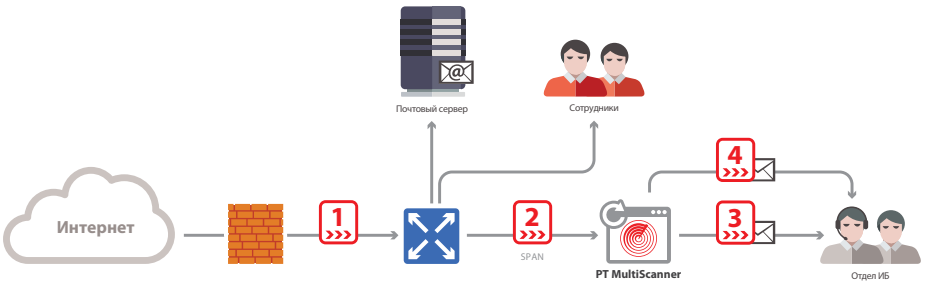
В целом, обеспечивая контроль трафика с помощью PT MultiScanner, организации получают возможность:

- проверять файлы из сетевого трафика в режиме реального времени;
- быстро получать вердикты по хеш-суммам файлов;
- проводить ретроспективный анализ и получать данные о вредоносном содержимом в ранее загруженных файлах;
- выявлять ботов во внутренней сети;
- оперативно реагировать на инциденты безопасности и блокировать распространение вредоносного контента, расследовать инциденты;
- передавать дополнительные события в системы защиты, в том числе SIEM и IPS/IDS.

Пассивный режим. PT MultiScanner прослушивает зеркалированный трафик от сети оборудования, поддерживающего технологию SPAN (Switch Port Analyzer). Данный вариант использования хоть и не предотвратит передачу вредоносного объекта, но сможет своевременно сигнализировать об угрозе.

Система не влияет на производительность сети, а также не требует больших трудозатрат при развертывании.

Для веб-ресурсов и файлов (например, передаваемых по протоколам HTTP и SMTP) выполняются статический анализ и фильтрация по черным спискам.



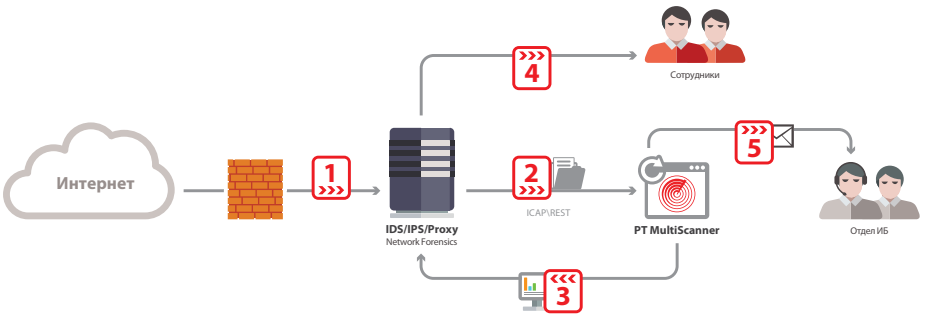
Организация сервиса контроля трафика

Сервис предполагает следующий сценарий использования:

1. Объект, поступающий внутрь сети по незашифрованным протоколам, проходит через сетевое оборудование, поддерживающее технологию SPAN.
2. Сетевое оборудование зеркалирует весь трафик, включая проверяемый объект, в систему PT MultiScanner.
3. В случае если система обнаружила вредоносные программы или файлы по результатам статического анализа и анализа по репутационным сервисам — формируется уведомление для отдела ИБ.
4. По заранее составленному расписанию PT MultiScanner перепроверяет объект после обновления антивирусных баз или базы знаний PT-индикаторов. Если предыдущий вердикт не подтвердится и объект будет признан зловредным, система сформирует для отдела ИБ уведомление об инциденте.

Активный режим. PT MultiScanner можно использовать на границе контролируемого периметра, интегрируя со средствами анализа трафика — для повышения общего уровня безопасности. В качестве средств анализа трафика могут выступать системы обнаружения и предотвращения вторжений (IDS, IPS), прокси-серверы и другие средства, поддерживающие протоколы ICAP, REST. Интеграция позволит настроить проверку всех файлов, загруженных с внешних подсетей (включая HTTPS) в автоматическом режиме.

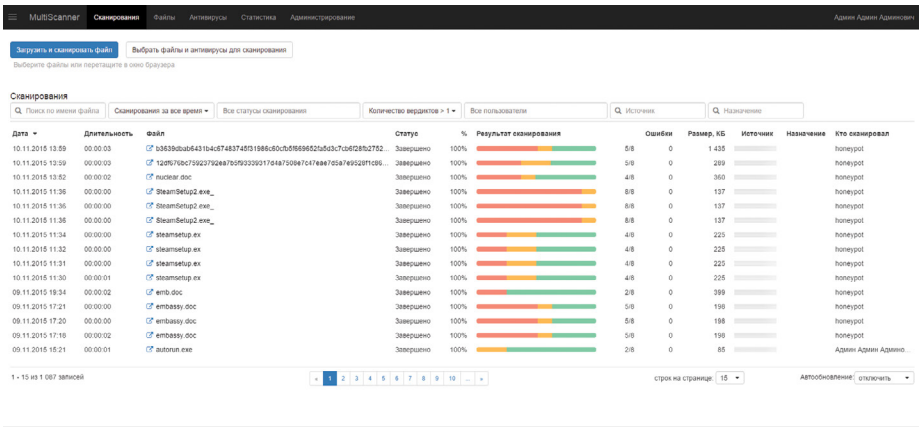
Данный вариант использования системы предотвратит передачу пользователям вредоносных файлов или программ.



Организация сервиса защиты периметра

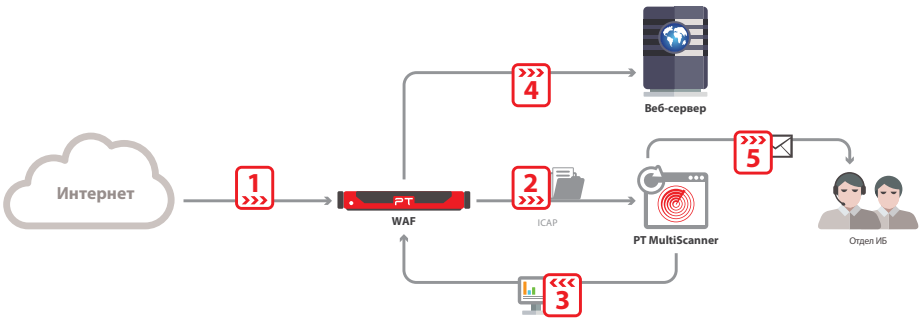
Один из сценариев работы системы на примере прокси-сервера:

1. Пользователь, скачивая файл из внешних подсетей, инициирует процесс его загрузки прокси-сервером.
2. После загрузки прокси-сервер перенаправляет файл для проверки в систему PT MultiScanner вместе с дополнительной информацией о пользователе и источнике загрузки.
3. Результаты сканирования отправляются на прокси-сервер в соответствующем формате.
4. Если файл не заражен, он перенаправляется пользователю, в противном случае — блокируется с последующим уведомлением пользователя и отдела ИБ.
5. В случае если вредоносное содержимое в файле было найдено при ретроспективном анализе после обновления антивирусных баз или репутационных сервисов, PT MultiScanner отправляет автоматическое уведомление об инциденте отделу ИБ.



3.3. Защита веб-приложений и порталов

PT MultiScanner применяется и для защиты веб-приложений и порталов. Сервис настраивается на контроль важнейших каталогов этих ресурсов или используется совместно с решениями для защиты веб-приложений (WAF), в том числе с продуктом компании Positive Technologies — Application Firewall. Для этого решение устанавливается внутри контролируемого периметра и интегрируется с WAF посредством протоколов ICAP или REST. Такая интеграция позволит проверять загружаемый контент и защищать веб-приложение от внешних угроз.



Использование PT MultiScanner совместно с PT Application Firewall

Сценарий работы системы при интеграции с PT Application Firewall:

1. Application Firewall контролирует весь трафик, направленный на веб-сервер.
2. После получения объекта PT AF перенаправляет его для проверки на вредоносное содержимое в PT MultiScanner, вместе с дополнительной информацией об источнике загрузки.
3. После сканирования объекта в систему Application Firewall возвращается вердикт проверки.
4. Если объект не заражен, он перенаправляется на веб-сервер; в противном случае объект блокируется с соответствующим уведомлением отдела ИБ.
5. По расписанию PT MultiScanner перепроверяет объект после обновления антивирусных баз или репутационных сервисов. Если прошлый вердикт не подтвердится и объект будет признан инфицированным, система сформирует уведомление об инциденте.

В конечном итоге организации получают:

+ защиту веб-приложения и пользователей от вредоносного контента,
+ контроль загружаемых пользователями файлов,
+ предотвращение утечек конфиденциальных данных, в том числе через веб-ботов,
+ детектирование и блокирование вредоносных программ и файлов.

А при совместном использовании PT MultiScanner и Application Firewall:

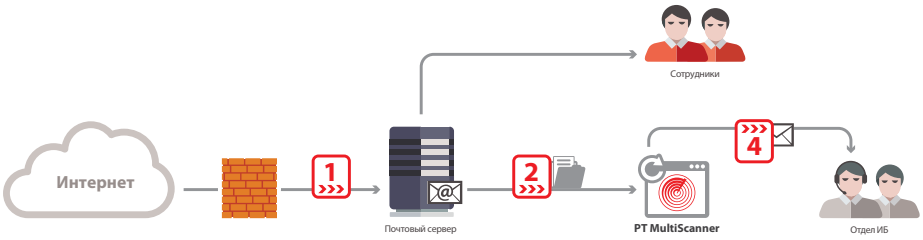
- блокирование 75% атак нулевого дня «из коробки»,
- самообучение и виртуальный патчинг,
- обнаружение и предотвращение фрода.

3.4. Контроль почтовых вложений (интеграция с почтовой системой)

С помощью PT MultiScanner можно выполнять автоматическое сканирование вложений на сетевом уровне. Для этого система устанавливается внутри контролируемого периметра и интегрируется с почтовыми серверами.

Этот вариант использования позволяет организациям обеспечить:

- онлайн-проверку почтовых сообщений на внешних и внутренних почтовых серверах,
- выявление вредоносных вложений и источников рассылки,
- выявление потенциально вредоносных ссылок во вложениях,
- периодическую перепроверку хранимых вложений почтовых сообщений,
- защиту против отдельных методов социальной инженерии.



Организация сервиса контроля почтовых вложений

Сценарий работы системы:

1. На почтовый сервер поступает сообщение с вложением.
2. PT MultiScanner загружает файл вложения вместе с дополнительной информацией, полученной на почтовом сервере из поля сообщения (от кого, кому, копия, тема).
3. PT MultiScanner производит сканирование объекта.
4. В случае если вредоносное содержимое в файле было найдено при первичном сканировании или при ретроспективном анализе после обновления антивирусных баз или репутационных сервисов, PT MultiScanner отправляет автоматическое уведомление об инциденте отделу ИБ.

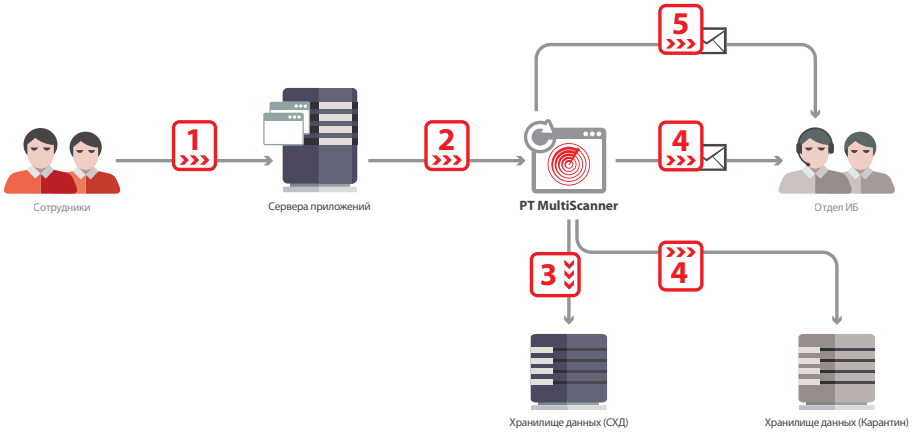
3.5. Контроль файловых хранилищ

Сервис контроля файловых хранилищ устанавливается внутри контролируемого периметра и предназначен для проверки файлов, находящихся на общедоступных ресурсах. Это позволяет осуществлять регулярное сканирование объектов на сетевых ресурсах и сигнализировать в случае появления вредоносных программ и файлов — для предотвращения распространения заражения в сети.

Этот вариант использования позволяет организациям:

- выявлять вредоносные программы и файлы, зараженные дистрибутивы и документы,
- оперативно реагировать на инциденты и блокировать распространение вредоносных файлов,
- проводить ретроспективный анализ и выявлять угрозы без пересканирования исходного файла,
- проводить плановые осмотры в периоды снижения сетевого трафика, чтобы снизить нагрузку в часы пик.

Кроме варианта мониторинга общедоступных ресурсов возможна проверка файлов, передаваемых для проверки в заданную входную папку PT MultiScanner. В зависимости от вердикта PT MultiScanner переложит исходный файл в заданную выходную папку или в папку карантина.



Организация сервиса контроля файловых хранилищ

Сценарий работы системы:

1. Пользователь загружает объект на сетевой ресурс.
2. PT MultiScanner загружает этот объект для проверки.
3. Если система не обнаружила вредоносное содержимое, то исходный файл будет переложен в заданную выходную папку (хранилище).
4. Если система обнаружила вредоносное содержимое, то исходный файл будет переложен в папку карантина, а для отдела ИБ сформировано соответствующее уведомление.
5. По расписанию PT MultiScanner перепроверяет объект после обновления антивирусных баз или репутационных сервисов. Если прошлый вердикт не подтвердится и объект будет признан инфицированным, система сформирует уведомление об инциденте.

4. PT MULTISCANNER: ВАРИАНТЫ ПОСТАВКИ

PT MultiScanner может быть развернут как программное, программно-аппаратное или виртуальное решение.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

POSITIVE TECHNOLOGIES

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays