POSITIVE TECHNOLOGIES

Построение центра ГосСОПКА

Комплексное решение для создания центра ГосСОПКА и взаимодействия с НКЦКИ

Строительство центра ГосСОПКА — длительный и трудоемкий процесс, поэтому мы предлагаем создавать его поэтапно. Это дает возможность организациям постепенно развивать внутреннюю экспертизу ИБ, выстраивать процессы в подразделении ИБ и успешно отражать как типовые атаки, так и новые их виды.

В основе решения лежат **продукты Positive Technologies**, с помощью которых служба ИБ сможет самостоятельно реализовать функции центра ГосСОПКА, а также **услуги экспертного центра безопасности Positive Technologies** (PT ESC). Специалисты PT ESC дополнят команду центра недостающей экспертизой и возьмут на себя сопровождение работы подразделения ИБ, в том числе часть функций центра ГосСОПКА.

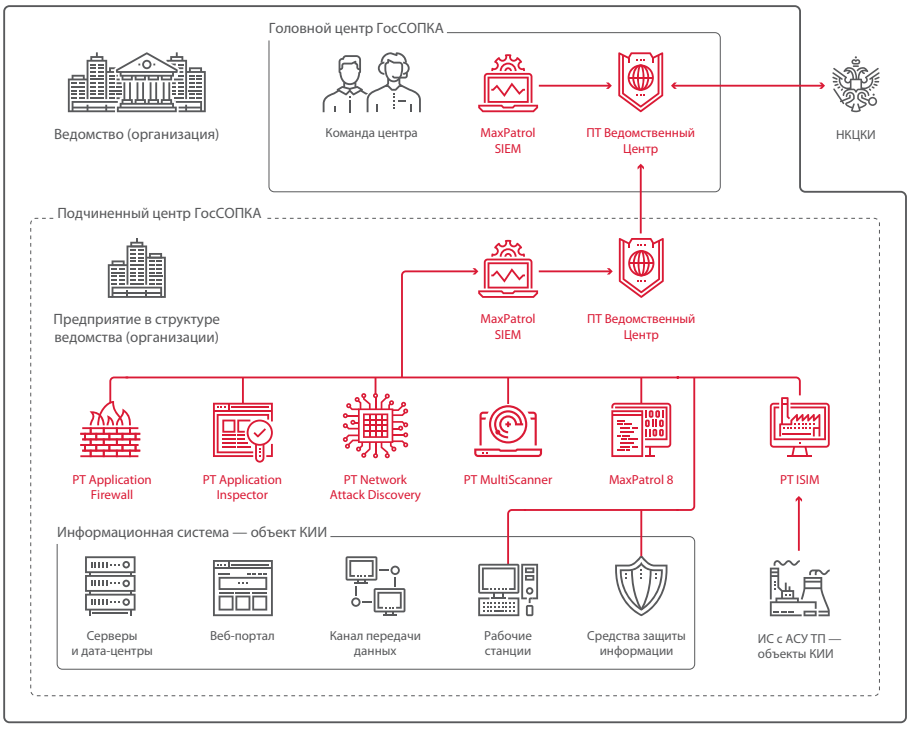
	Стадия 1: защита от типовых атак на периметр	**Стадия 2: защита от типовых внутренних атак**	**Стадия 3: защита от нетиповых атак**
САМОСТОЯТЕЛЬНО РЕАЛИЗУЕМЫЕ ФУНКЦИИ	• Инвентаризация внешних информационных систем (ИС) — **MaxPatrol 8** • Анализ типовых уязвимостей — **MaxPatrol 8** • Обнаружение атак на внешние веб-интерфейсы ИС — **PT Application Firewall**	• Анализ событий безопасности и выявление инцидентов — **MaxPatrol SIEM** • Инвентаризация внутренних ИС — **MaxPatrol 8** • Анализ сетевого трафика — **PT Network Attack Discovery** • Обнаружение атак в АСУ ТП — **PT ISIM** • Взаимодействие с НКЦКИ — **«ПТ Ведомственный центр»**	• Расследование инцидентов — **MaxPatrol SIEM** и другие техсредства ГосСОПКА • Анализ исходного кода — **PT Application Inspector** • Ретроспективный и динамический анализ вредоносного ПО на потоке — **PT MultiScanner** • Оценка соответствия стандартам — **MaxPatrol 8**
АУТСОРСИНГ СЕРВИСОВ ЭКСПЕРТАМ PT ESC	• Контроль защищенности сетевого периметра — **сервис PT Advanced Border Control** • Экспертный анализ уязвимостей внешних ИС • Анализ событий безопасности для внешних ИС • Реагирование на компьютерные атаки • Взаимодействие с НКЦКИ	• Экспертный анализ уязвимостей • Реагирование на неизвестные компьютерные атаки	• Экспертный анализ уязвимостей • Реагирование на неизвестные компьютерные атаки
РЕЗУЛЬТАТ	Частично сформированы первая и вторая линия реагирования. Специалисты центра самостоятельно проводят первичную обработку инцидентов	Полностью сформированы первая и вторая линии реагирования. Специалисты центра реагируют на типовые кибератаки, проводят их расследование и взаимодействуют с НКЦКИ	Сформирована третья линия реагирования. Ведомственный (корпоративный) центр самостоятельно реализует все требуемые функции. Специалисты центра реагируют на новые виды угроз, проводят расследования, оказывают экспертную поддержку

ОСОБЕННОСТИ РЕШЕНИЯ

- **Быстрый старт выполнения требований.** Постепенное построение центра позволяет спланировать бюджет и уже на первом этапе начать выполнять требования законодательства и взаимодействовать с НКЦКИ.
- **Соответствие требованиям регуляторов на лету.** Продукты Positive Technologies регулярно обновляются с учетом актуальных угроз и требований новых нормативно-правовых актов.
- **Единая экосистема.** Все продукты являются частью универсальной платформы средств безопасности Positive Technologies, что обеспечивает совместимость компонентов и простоту интеграции.
- **Высокий уровень практической безопасности IT-систем.** Продукты Positive Technologies защищают критические IT-инфраструктуры крупнейших российских банков и промышленных предприятий, федеральных органов власти, госкорпораций.
- **Оперативное противодействие актуальным угрозам.** Эксперты PT ESC непрерывно анализируют актуальные угрозы и передают данные об уязвимостях, способах выявления и реагирования на новые типы атак в единую базу знаний Positive Technologies Knowledge Base, которая входит в MaxPatrol SIEM.

Подробнее о решении

Архитектура центра госсопка



Функции продуктов в центре ГосСОПКА

MaxPatrol SIEM	**Система мониторинга событий и выявления инцидентов ИБ** Ядро центра, проводит инвентаризацию ресурсов, анализирует события, выявляет инциденты и передает их в «ПТ Ведомственный центр».
MaxPatrol 8	**Система контроля защищенности** Анализирует защищенность, выявляет уязвимости, проводит инвентаризацию и отслеживает изменения в IT-инфраструктуре.
PT Application Firewall	**Межсетевой экран уровня приложений** Выявляет и блокирует атаки на веб-приложения, помогает в расследовании инцидентов.
PT Network Attack Discovery	**Система комплексного анализа сетевого трафика** Отслеживает и анализирует сетевой трафик, выявляет атаки, сетевые аномалии, скрытое присутствие, активности вредоносного ПО, в том числе в ретроспективе.
PT ISIM	**Система управления инцидентами кибербезопасности АСУ ТП** Осуществляет мониторинг защищенности АСУ ТП, выявляет кибератаки на ее компоненты и передает их в «ПТ Ведомственный центр».
PT MultiScanner	**Система выявления вредоносного контента** Выявляет вредоносное ПО, помогает в расследовании инцидентов заражения, позволяет проводить ретроспективный анализ.
PT Application Inspector	**Анализатор защищенности исходного кода приложений** Выявляет уязвимости исходного кода и готового веб-приложения.
«ПТ Ведомственный центр»	**Система управления инцидентами и взаимодействия с НКЦКИ** Позволяет реализовать процесс управления инцидентами, ведет учет инцидентов, передает данные в НКЦКИ.

О компании

Positive Technologies уже 19 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях (Facebook, ВКонтакте, Twitter), а также в разделе «Новости» на сайте ptsecurity.com.

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