КАЛИНИНГРАДСКАЯ ОБЛАСТЬ СТРОИТ РЕГИОНАЛЬНЫЙ ЦЕНТР КИБЕРБЕЗОПАСНОСТИ НА БАЗЕ РЕШЕНИЯ PT PLATFORM 187

«Перед нами стоит серьезная задача — оперативно построить один из первых региональных центров ГосСОПКА и обеспечить безопасность объектов КИИ органов власти Калининградской области. Благодаря комплексному решению PT Platform 187 за месяц удалось запустить центр безопасности и начать выполнение требований законодательства».

Сергей Чуприс, директор КГ НИЦ

ПРОФИЛЬ КОМПАНИИ

- **Название:** Калининградский государственный научно-исследовательский центр информационной и технической безопасности
- **Деятельность:** обеспечение информационной безопасности правительства области и оказание услуг удостоверяющего центра
- **Сайт:** kgnic.ru

- **Задача:** построить региональный центр безопасности для мониторинга событий ИБ в органах власти и подключения к ГосСОПКА
- **Решение:** PT Platform 187

Калининградский государственный научно-исследовательский центр информационной и технической безопасности (КГ НИЦ) оказывает услуги по защите персональных данных, аттестации объектов информатизации, выпуску сертификатов для электронных подписей и подготовке специалистов по ИБ. Ключевые заказчики — органы власти Калининградской области.

ЗАДАЧА

Согласно Федеральному закону № 187-ФЗ субъекты критических информационных инфраструктур (КИИ) обязаны обеспечивать безопасность значимых объектов. Если информационные системы государственного органа власти относятся к одной из 13 сфер, определенных в законе, то орган власти является субъектом КИИ.

Для помощи органам власти Калининградской области в вопросах защиты объектов КИИ и взаимодействия с ГосСОПКА правительство региона приняло решение о создании регионального центра компетенций в сфере информационной безопасности.

По предложению Агентства по развитию связи и массовых коммуникаций Калининградской области на базе КГ НИЦ будет построен **региональный центр безопасности** (security operations center, SOC) **со статусом центра ГосСОПКА**. В задачи SOC будут входить мониторинг событий ИБ, выявление и расследование инцидентов в информационных системах органов власти Калининградской области.

Создание регионального SOC — трудоемкая и дорогостоящая задача, которая требует развития экспертизы команды ИБ, формирования процессов, закупки и внедрения технических средств для обнаружения и предотвращения атак. Агентство по развитию связи и массовых коммуникаций совместно с КГ НИЦ решили **строить центр поэтапно**: распланировав бюджет, постепенно развивать архитектуру центра, отрабатывать процесс реагирования на атаки на небольших инфраструктурах и систематично расширять область мониторинга.

РЕШЕНИЕ

КГ НИЦ изучил программно-аппаратный комплекс PT Platform 187 для реализации основных требований 187-ФЗ и функций центров ГосСОПКА. Комплекс состоит из пяти технических средств Positive Technologies и предназначен для небольших инфраструктур — до 250 сетевых узлов.

PT Platform 187 — ПАК для реализации основных функций безопасности значимых объектов КИИ и подключения к ГосСОПКА.

Пять продуктов в одном:

- система выявления инцидентов MaxPatrol SIEM,
- система контроля защищенности MaxPatrol 8,
- система выявления следов компрометации в сетевом трафике PT Network Attack Discovery,
- многоуровневая система защиты от вредоносного ПО — PT MultiScanner,
- система управления инцидентами и взаимодействия с ГосСОПКА «ПТ Ведомственный центр»

Для небольших инфраструктур: подходит инфраструктурам до 250 сетевых узлов и территориальным подразделениям как часть сегмента ГосСОПКА

Быстрое внедрение: 30 дней занял ввод продукта в промышленную эксплуатацию в КГ НИЦ

Решение подходило под задачи КГ НИЦ, поскольку:

- **Позволяет выполнить требования законодательства.** PT Platform 187 помогает реализовать задачи обеспечения защиты КИИ в части аудита безопасности, антивирусной защиты на потоке, обнаружения вторжений, анализа сетевого трафика, выявления инцидентов и реагирования на них, взаимодействия с ГосСОПКА.
- **Автоматизирует процессы ИБ.** Продукты в составе PT Platform 187 интегрированы между собой, что помогает максимально снизить ручное вмешательство администратора.
- **Может быть масштабировано.** Для подключения к PT Platform 187 более 250 сетевых узлов предусмотрен постепенный переход на enterprise-версии продуктов, входящих в ПАК.
- **Соответствует политике импортозамещения.** Решение PT Platform 187 разработано на базе отечественных продуктов.

Внедрение PT Platform 187 заняло месяц. Специалисты КГ НИЦ подготовили сетевую инфраструктуру для развертывания решения и установили сервер PT Platform 187. Инженеры Positive Technologies с помощью специалистов КГ НИЦ настроили компоненты системы и провели опытную эксплуатацию. К решению были подключены информационные системы министерств в сферах науки, здравоохранения, промышленности.

Ядро платформы — MaxPatrol SIEM — формирует детальную модель IT-инфраструктуры, которая постоянно обогащается сведениями о конфигурации, уязвимостях, программном и аппаратном обеспечении информационных ресурсов из системы контроля защищенности MaxPatrol 8 и анализатора сетевого трафика PT Network Attack Discovery.

На основе данных из источников, в том числе из PT Network Attack Discovery и системы защиты от вредоносного ПО PT MultiScanner, MaxPatrol SIEM выявляет инциденты. Информация об инциденте автоматически передается в «ПТ Ведомственный центр» для регистрации и реагирования.

Помимо выявления атак, с помощью PT Platform 187 региональный центр безопасности на базе КГ НИЦ выполняет следующие задачи:

- непрерывно инвентаризует информационные ресурсы и автоматически обновляет сведения об инфраструктуре;
- в соответствии с выбранной периодичностью проводит анализ защищенности и выявляет уязвимости; получает отчет по результатам аудита и информацию о соответствии стандартам безопасности;
- предотвращает распространение вредоносного ПО;
- контролирует и анализирует сетевой трафик до уровня L7 включительно;
- обрабатывает инциденты и помогает управлять процессом реагирования в соответствии с методическими рекомендациями ФСБ России по созданию центров ГосСОПКА.

РЕЗУЛЬТАТЫ И ПЛАНЫ

PT Platform 187 стала основой регионального центра безопасности, формируемого в Калининградской области на базе КГ НИЦ. Благодаря этому решению КГ НИЦ отслеживает события ИБ в подключенных системах и выявляет атаки. До конца 2018 года центр планирует организовать подключение к ГосСОПКА для передачи информации об атаках на объекты КИИ региональных органов государственной власти.

Постепенно центр будет расширять область мониторинга и переходить на enterprise-версии продуктов, входящих в PT Platform 187. В 2019 году к центру будут подключены 1000 сетевых устройств органов власти Калининградской области, а к 2020 году — все 3000 устройств. Таким образом SOC станет единым центром кибербезопасности в регионе.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. 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.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

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