

Исх. № 36-КГ НИЦ от 11.02.2021г.

Генеральному директору АО «Позитив  
Текнолоджиз»

Ю.В. Максимову

Уважаемый Юрий Владимирович!

«Калининградский государственный научно-исследовательский центр информационной и технической безопасности» (КГ НИЦ) использует систему анализа трафика и выявления атак PT Network Attack Discovery с 2018 года. Тогда мы начинали строить региональный центр безопасности (security operations center, SOC) для защиты органов государственной власти Калининградской области от хакерских атак. С 2020 года SOC функционирует как государственная информационная система «Центр управления безопасностью».

Незаменимой частью центра стал PT NAD. Он дает специалистам SOC около 70% полезной информации об инцидентах, выявленных в органах власти Калининградской области. Нам нравится, что он глубоко разбирает трафик и детально отображает, что происходит в подключенных к мониторингу сетях. Несколько серьезных инцидентов мы выявили благодаря сигналам в PT NAD о подозрительных соединениях.

Вместе со специалистами PT Expert Security Center мы оперативно расследовали сложные запутанные атаки на региональные органы власти и приняли меры по предотвращению их развития.

Надеемся на продолжение плодотворного сотрудничества в области кибербезопасности.

С уважением,

и.о. директора



А.А. Персичкин