"ИнфоТеКС" подключил первый регион к ГосСОПКА

Издание: ComNews, июль 2019 г.
Спикер: Иван Мелехин, директор по развитию

Подробнее: https://www.comnews.ru/content/120767/2019-07-12/infoteks-podklyuchil-pervyy-region-k-gossopka?fbclid=IwAR2FwAElY8nvhz-w4eNmpHShsMmlNmDR16T5SCW01sdQXT_Hiu4FQjsZbac

ГК "ИнфоТеКС" подключила первый в России субъект РФ - Республику Тыва к Государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Это первое подключение субъекта РФ через сторонний центр ГосСОПКА с использованием технической инфраструктуры Национального координационного центра по компьютерным инцидентам (НКЦКИ).

Как сообщила компания "ИнфоТеКС", в настоящее время к системе подключены информационные ресурсы ключевых органов государственной власти. Среди них такие, как администрация главы и аппарат правительства Республики Тыва, министерства финансов, экономики и юстиции, Министерство по регулированию контрактной сферы в сфере закупок, Управление делами правительства и Агентство по внешнеэкономическим связям. На очереди к подключению к ГосСОПКА - Министерство информатизации и связи Республики Тыва, Центр информационных технологий, а также ряд других региональных министерств и ведомств.

Как рассказали в "ИнфоТеКСе", для реализации задачи сети министерств и ведомств Тывы объединены в сеть передачи данных с одной точкой подключения к сетям международного обмена. "Трафик с границы сети зеркалируется и анализируется сенсором средства обнаружения вторжений (СОВ) ViPNet IDS NS. Для сбора и анализа информации используется ПАК ViPNet TIAS. Информация об инцидентах анализируется в центре ГосСОПКА компании "Перспективный мониторинг" (входит в ГК "ИнфоТеКС") и передается в систему ГосСОПКА через техническую инфраструктуру НКЦКИ", - указывает подробности компания.

Реализация данного проекта отвечает Федеральному закону №187-ФЗ в части подключения субъектов критической информационной инфраструктуры (КИИ) к ГосСОПКА. Так, в Тыве появился ведомственный центр мониторинга инцидентов информационной безопасности. В его создании принимал участие интегратор систем информационной безопасности в регионе ГК "Грань безопасности". Это позволяет сотрудникам Управления защиты информации администрации главы Республики Тыва вовремя реагировать на инциденты сразу нескольких информационных ресурсов республиканских органов государственной власти.

По словам директора центра мониторинга и реагирования на кибератаки Solar JSOC компании "Ростелеком-Солар" Владимира Дрюкова, у "Ростелеком-Солара" также есть опыт как оказания услуг корпоративного центра ГосСОПКА (в этом случае организации подключаются к Главному центру через JSOC), так и построения таких центров в различных отраслях экономики - в органах государственной власти, энергетике, ТЭК. Часть проектов уже завершены, а другие находятся в процессе.

Среди недавних примеров Владимир Дрюков привел реализацию функций центра ГосСОПКА для правительства Самарской области в период проведения Чемпионата мира по футболу в 2018 г. "В зону ответственности Solar JSOC вошли выявление, анализ и выработка рекомендаций по реагированию на инциденты ИБ, анализ угроз и взаимодействие с Главным центром ГосСОПКА. Региональный центр кибербезопасности Самарской области взял на себя работы по оперативному реагированию и

ликвидации последствий возможных инцидентов. За это время экспертная команда выявила и отразила более 150 сложных, развивающихся во времени атак. Количество базовых инцидентов ИБ в Самаре во время проведения ЧМ-2018 составило более 1000", - рассказал он.

Менеджер по развитию бизнеса "Лаборатории Касперского" Алексей Киселев подчеркивает, что "Лаборатория Касперского" не является и не планирует становиться коммерческим центром ГосСОПКА. "Наша компания предлагает свои решения для построения SOC и реализации функционала ГосСОПКА - как при создании собственного сегмента, так и при создании центра ГосСОПКА, коммерческого, ведомственного и т.д., - а также для реализации субъектами КИИ требований 230 приказа ФСТЭК по обеспечению безопасности значимых объектов КИИ", - говорит он.

Как замечает директор по развитию компании "Информзащита" Иван Мелехин, в последнее время мы наблюдаем экспоненциальный рост интереса к теме КИИ и взаимодействия с ГосСОПКа. "Благодаря действиям регуляторов и ужесточению ответственности практически каждый субъект КИИ в настоящее время озабочен выполнением соответствующих требований, - говорит он. - Необходимо отметить, что большинство субъектов в настоящий момент находятся в стадии категорирования объектов и разработки планов защиты и только начинают задумываться о подключении к ГосСОПКА. При этом, согласно закону, любой субъект КИИ должен обеспечить подключение к ГосСОПКа вне зависимости от степени завершения работ по обеспечению соответствия, что предполагает не только наличие развернутых и работающих средств защиты, но и ряда специфичных сервисов, например таких, как анализ данных о событиях информационной безопасности, выявление и реагирование на кибератаки, анализ уязвимостей и многое другое".

При этом, замечает специалист "Информзащиты", развернуть подобный комплекс крайне сложно и затратно не только с технической стороны. Он сетует, что одной из основных проблем является острая нехватка квалифицированных специалистов. "Для клиентов наиболее популярным решением с разумным бюджетом является передача этих функций на аутсорсинг таким специализированным центрам, как "Перспективный мониторинг" или IZ:SOC (SOC "Информзащиты"), которые берут на себя большую часть проблем, связанных с реализацией требований законодательства", - говорит Иван Мелехин.

На эту же проблему указывает и директор по методологии и стандартизации Positive Technologies Дмитрий Кузнецов. "Основная трудность в процессе определения объектов КИИ заключается в нехватке на рынке труда РФ квалифицированных специалистов, компетентных в вопросах противодействия компьютерным атакам. Таких людей катастрофически мало, и их подготовка сейчас превращается в задачу государственной значимости", - говорит он.

По оценкам специалиста "Информзащиты", минимальный бюджет реализации специфических требований для подключения ГосСОПКи может составлять десятки миллионов рублей. "Чем выше степень зрелости системы информационной безопасности организации, тем меньше могут быть затраты, - поясняет он. - Если в организации развернуты средства защиты в соответствии с разработанными моделями угроз, есть средства мониторинга, квалифицированный персонал - то процесс подключения может быть существенно упрощен. Если организация больший упор делала на развитие ИТ для поддержания бизнеса, то капитальные вложения на реализацию требований могут быть очень значительными, и в этом случае опять на помощь могут прийти корпоративные центры ГосСОПКа, например наш IZ:SOC".

Аналитик ГК InfoWatch Андрей Арсентьев полагает, что процесс определения объектов критической информационной инфраструктуры тормозится на местах, несмотря на то что в последнее время чувствуется положительная динамика. "Главная проблема составления перечня объектов КИИ - точное категорирование соответствующих объектов, то есть разнесение объектов по трем категориям значимости: 3-1, 1 - максимальная, - указывает он. - Категорирование идет довольно медленно, потому что для части компаний это сложно и дорого, а еще у части просто нет стимулов со стороны государства. В итоге этот непростой, требующий длительного аудита процесс корпорации

откладывают в долгий ящик, а потом и вовсе - спускают на тормозах, что создает реальные угрозы их безопасности". Так, по данным ФСТЭК, на которые ссылается Андрей Арсентьев, на начало 2019 г. полноценное категорирование прошли только около 15% субъектов КИИ.

Как поясняет аналитик InfoWatch, не меньше проблем с процессом определения объектов КИИ ожидается и на втором этапе, когда компаниям, у которых есть немало таких объектов, нужно будет формировать модели угроз и подключать средства защиты. "Вообще, только имея полностью охваченную системой ГосСОПКА карту объектов КИИ, крупные корпорации из ТЭК, финансового, логистического сектора и других системообразующих отраслей смогут точно и полно представлять картину атак на эти важные объекты", - подчеркивает он.

Специалист "Ростелеком-Солара" уверен, что категорирование инфраструктур ведется очень активно во всех отраслях. "Наибольшую сложность испытывают компании, которым необходимо проводить аудиты не только корпоративных и закрытых сегментов ИТ-ландшафта, но и технологических процессов, а также обеспечивать их безопасность. Несмотря на то что направление безопасности АСУ ТП зародилось уже достаточно давно, реального практического опыта и у клиентов, и у компаний-партнеров здесь значительно меньше, чем в сфере обеспечения ИБ корпоративных инфраструктур", - указывает он.

Как отмечает специалист "Лаборатории Касперского", по мере появления не только рекомендуемых, но и предписывающих сроков проведения процессов определения объектов, категорирования и т.д. процесс набирает более активный ход. Ранее, добавляет он, многие потенциальные субъекты КИИ просто игнорировали рекомендуемые сроки выполнения работ.

Специалист Positive Technologies уверяет, что ведомственные центры ГосСОПКА сейчас создаются во многих федеральных органах исполнительной власти и органах власти субъектов Федерации. Для их построения используются типовые решения, в том числе и на основе продуктов компании. Например, Калининградская область строит региональный центр кибербезопасности на базе PT Platform 187. "Программно-аппаратный комплекс PT Platform 187 стал основой формируемого в Калининградской области регионального центра безопасности. Задача центра - помогать органам государственной власти Калининградской области в вопросах защиты объектов КИИ", - пояснил он.

Коммерческий сектор в этом отношении отстает: если для органов власти постановлением правительства установлен жесткий срок завершения категорирования (они должны составить перечни объектов КИИ к 1 сентября 2019 г. и завершить категорирование к 1 сентября 2020 г.), то, как указывает специалист Positive Technologies, у коммерческих компаний таких временных рамок нет. "Поэтому в том, что касается практического противодействия атакам они идут по другому пути: создают свои, корпоративные центры реагирования на атаки - Security Operations Center, SOC - для решения собственных задач и лишь потом подключают их к инфраструктуре НКЦКИ. При этом в обоих случаях используются примерно одинаковые технические решения", - говорит он.

Директор центра компетенций по информационной безопасности компании "Техносерв" Сергей Терехов указывает на то, что направление защиты КИИ является одним из ключевых направлений "Техносерва" в области информационной безопасности. "В частности, сейчас завершаем крупный проект по категорированию объектов КИИ в восьми промышленных предприятиях, находящихся в пяти субъектах РФ. Уже определены критические процессы, значимые объекты КИИ и их категории значимости, разработаны внутренние нормативные документы по защите объектов КИИ, спроектированы технические решения по защите объектов КИИ", - рассказывает он.

В последние несколько месяцев "Техносерв" замечает увеличение интереса к теме выполнения требований по КИИ и подключения к ГосСОПКЕ. "В первую очередь это связано с тем, что не так давно законодательно была определена дата подачи сведений об объектах КИИ во ФСТЭК России - 1 сентября 2019 г. для субъектов - государственных органов и государственных учреждений. Также все больше субъектов КИИ занимаются этим вопросом. Нормативные документы выпущены, сроки есть,

правила государственного контроля в области обеспечения безопасности КИИ утверждены, проверки близятся", - отмечает он.

Некоторые аспекты, продолжает специалист "Техносерва", требуют дополнительных усилий. "Во-первых, не все смогли разобраться в правилах категорирования объектов КИИ и правилах определения значений показателей критериев значимости объектов КИИ. Во-вторых, возникает очень много организационных нюансов. Например, для категорирования объектов КИИ нужно создать комиссию. Состав комиссии, с одной стороны, определен в ПП РФ №127, с другой стороны, он требует, чтобы члены комиссии были работниками субъекта КИИ. Однако есть организации, которые определенные задачи отдали на аутсорсинг. Например, требуется в составе комиссии иметь человека из ИТ, но ИТ обслуживает сторонняя организация - или организация из группы компаний, в которую входит субъект. Алгоритмы для некоторых случаев не прописаны. В-третьих, возникают проблемы взаимодействия различных подразделений. Категорирование объектов КИИ - достаточно сложный процесс, требующий участия специалистов из разных областей - ИТ, ИБ, службы автоматизации, финансовые подразделения, ГОиЧС и др. Собрать всех вместе и выработать единое решение - задача непростая, решаемая, но требующая порой очень много времени", - перечисляет Сергей Терехов.

Что касается необходимых методических рекомендаций, регулирующих правила создания и подключения к ГосСОПКА, то, как отмечает Алексей Киселев, они есть. В компании "Информзащита" уточнили, что вышел Приказ ФСБ России от 06.05.2019 №196 "Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты".