Ситуационные центры безопасности:

митигация рисков и способность адаптации к новым угрозам

Большинство современных промышленных корпораций в настоящее время представляют собой не столько монопрофильное предприятие, сколько мультиотраслевой конгломерат, включающий объекты как производственной, транспортной, логистической инфраструктуры, так и социального и культурного назначения. Обеспечение безопасности и непрерывности как собственно производственных, так и иных процессов, входящих в контур компании, требует и новых решений – как организационного, так и технологического уровня. По сути, основные участники индустриального сектора начинают формировать корпоративные экосистемы безопасности – институциализированное решение, позволяющее гибко и оперативно адаптировать имеющиеся ресурсы новым вызовам и угрозам. Одним из ключевых элементов формирующихся корпоративных экосистем становятся ситуационно-аналитические центры безопасности (САЦБ). Об опыте разработки и внедрения системы САЦБ, рисках и перспективах ее развития рассказывает начальник Управления проектов объектовой безопасности ПАО «ГМК «Норильский никель» Максим МАЛОВ.

«Вопросы обеспечения безопасности объектов ПАО «ГМК «Норильский никель» как организации с разветвленной географической структурой, расположенной в том числе в Арктической зоне, носят приоритетный характер и требуют оперативного управления для обеспечения стабильности производственных процессов.

В условиях действующих международных ограничений, коснувшихся многих российских компаний, роль таких стратегических предприятий, как «Норникель», в формировании бюджета страны усиливается. Соответственно, растет цена рисков, возникающих в результате реализации актов незаконного вмешательства.

Бизнес-модель «Норникеля» включает в себя 4 ключевых этапа:

- Минерально-сырьевая база и геологоразведка.
- Добыча и производство металлов.
- Энергетическая база, добыча и подготовка газа и газового конденсата.
- Логистика и сбыт.
- Научная работа/разработка новых технологий/материалов.

Энергетическая обособленность, географическая и климатическая дифференцированность территорий, где работает Компания, определяет подходы к обеспечению защиты объектов.

Обеспечение плановой бесперебойной работы всех производственных, финансовых, логистических, информационных и т. д. цепочек предприятий «Норникеля» и организаций корпоративной структуры, поддержание социальной стабильности в регионах присутствия – основные требования бизнеса к Блоку корпоративной защиты Компании.

Именно в таком формате организована и функционирует система корпоративной безопасности «Норникеля», созданная для защиты законных интересов компании практически во всех сегментах ее деятельности.

Эффективность реализации мероприятий по обеспечению защищенности объектов достигается за счет взаимодействия с профильными органами государственной власти как на региональном, так и федеральном уровнях, в рамках которого реализуются требования основных федеральных нормативных правовых актов: законов Российской Федерации № 35-ФЗ «О противодействии терроризму», № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса», № 16-ФЗ «О транспортной безопасности», постановления Правительства РФ № 258 «Об утверждении требований к антитеррористической защищенности объектов (территорий) промышленности…».

В рамках реализации базового документа стратегического планирования «Норникеля» – Комплексной программы развития объектовой безопасности – в настоящее время реализовано и на разных стадиях реализации более 100 инвестиционных проектов Компании и организаций корпоративной среды на территории от Кольского полуострова до Забайкальского края.

В целях создания единого информационного пространства безопасности, консолидации информационно-аналитической системы, эффективно реагирующей на угрозы в области объектовой безопасности, создания эффективного современного инструмента обеспечения объектовой и антитеррористической безопасности объектов Компании выполняются мероприятия по созданию системы ситуационно-аналитических центров безопасности (ССАЦБ).

Система САЦБ призвана замкнуть единый контур информационной среды безопасности Компании и вывести его на новый качественный уровень за счет создания и постоянной актуализированной системы знаний в области обеспечения объектовой, промышленной и экологической безопасности, ликвидации нештатных ситуаций путем формирования всесторонней аналитической среды, «банка сценариев» действий как при наступлении «тревожных» событий, так и в прогнозных целях.

Скорость получения и обработки информации, скорость принятия решений и скорость реагирования, прогнозирование ситуаций на основе цифровых моделей угроз становятся концептуальной основой работы подразделений безопасности уже сейчас и на перспективу.

Сегодня создан и активно развивается Главный ситуационно-аналитический центр Компании с локацией в Москве. К нему подключены ресурсы безопасности Красноярска и Мурманска. Завершено формирование регионального САЦБ в Кольской ГМК, на завершающем этапе создание САЦБ в Заполярном филиале Компании в Норильске.

Вскоре они будут передавать информацию в Главный ситуационный центр. В результате все объекты и транспорт «Норникеля» будут мониториться в режиме реального времени. Таким образом мы автоматизируем процессы, минимизируем влияние человеческого фактора и оптимизируем расходы. А в итоге – усиливаем защиту корпоративной инфраструктуры в интересах Компании.

Создание системы САЦБ планируется по Гибридной схеме.

Эта концепция предполагает интеграцию централизованной и децентрализованной архитектур построения, допуская:

- автономное размещение вычислительных и программных ресурсов для логистических площадок на территории первого (Главный САЦБ) и второго (Региональный САЦ) уровней;
- создание узловой централизованной логистической площадки в ГСАЦ, обеспечивающей сбор данных с объектов 3 уровня (ССОИ/ИСБ) без развертывания в них автономных вычислительных ресурсов с последующей возможностью предоставления данных на второй уровень (РСАЦ).

Логистическая архитектура платформы строится из следующих элементов:

- основное веб-приложение с использованием технологии, позволяющей непрерывно взаимодействовать с остальными компонентами Системы. Она позволяет реализовать функционал уведомлений о событиях в системе, работы со слоями объектов на геоинформационной карте, маршрутизации запросов к сторонним серверам. Такое решение позволит обеспечить основной функционал: авторизацию работы со слоями на картографической подложке, отображения данных в различных форматах, отображение видеопотоков и т. д.;
- программная платформа, реализующая функционал обработки запросов пользователей к СУБД Системы, выполнения расчетных задач, ведения журнала действий пользователей, формирования перечня объектов на карте, создания событий, инцидентов, неисправностей, поручений при получениях сообщений от систем мониторинга, формирования отчетов и экспортов, а также выполнения задач по расписанию с применением планировщика.

Данная логистическая архитектура позволит создать единое информационное пространство в Группе компаний «Норильский никель» посредством подключения различных источников данных и оконечных устройств в единую информационную среду; структурирование и формализацию данных с целью создания прикладных аналитических сервисов, решающих поставленные задачи.

Подсистемы САЦ:

- мониторинг безопасности;
- географическая информационная;
- справочная;
- сервисная;
- информационно-аналитическая;
- сторонние информационные системы и сервисы.

Кроме того, для оперативного управления система предусматривает организацию как внутренней, так и внешней видеоконференцсвязи.

Внедрение системы ситуационно-аналитических центров

безопасности предоставило нам новые возможности по мониторингу, контролю и управлению процессами в части безопасности Компании. Многие процессы, ранее требующие огромного количества человеческих усилий, после перевода их в «цифру» дали значительный прирост производительности при снижении человеческих усилий. Такой сферой, к примеру, стала автоматизация и консолидация данных о техническом состоянии оконечного оборудования. Ранее каждый объект самостоятельно силами сотрудников охраны отслеживал, выявлял и фиксировал факты неисправности ИТСО. Передача информации в службы технической поддержки происходила в формате заявок по телефону или по электронной почте, включался традиционный регламент, не позволявший быстро определить, в какой стадии находится заявка, срок ее исполнения и ответственного. Внедрение единого автоматического инструмента контроля и отработки неисправностей ИТСО позволило снять часть нагрузки с сотрудников охраны.

Большой объем информации в систему может поступать от автоматических подсистем контроля доступности оборудования. Такой переход позволил выявить как точки роста в техническом оснащении (на ряде объектов при проектировании периметральных систем охраны недостаточно учитывались ветровые и снеговые нагрузки на ограждения), так и специфические особенности функционирования оборудования различных производителей. Ранее отдельные сигналы от ТСО на объектах не приводили к возникновению стратегического пересмотра использования оборудования. Но когда данные от множества объектов слились в единый поток информации, то ощутимые отклонения в работе ИТСО с едиными характеристиками дали сигналы к развитию и пересмотру подходов в оснащении в целом.

Вовлечение в информационное обеспечение системы ситуационно-аналитических центров безопасности информационных потоков от смежных направлений деятельности компаний привело к симметричной заинтересованности коллег. Совместная информационная работа приводит к перестройке маршрутов и порядка внутреннего взаимодействия в Компании. Функция безопасности в компании становится инициатором развития процессов в иных направлениях Компании.

Как любая информационная система, САЦ нашей Компании эволюционировал в несколько этапов и продолжает развиваться. В начале своего пути ситуационный центр вбирал в себя данные от комплексных систем безопасности и предоставлял автоматизацию отработки ситуаций, связанных исключительно с сигналами тревог. Создаваемый комплекс обеспечивает автоматизацию многих процессов, ранее выполнявшихся в ручном режиме.

Развитием системы стало вовлечение в процесс автоматизации дополнительных направлений обеспечения безопасности, таких как информационные потоки о событиях, фиксируемых персоналом направления безопасности Компании.

Наиболее ценным ресурсом в части машинного обучения и внедрения предиктивных и генеративных подходов является регулярный и систематизированный сбор данных. Технические средства охраны, информация из открытых источников (СМИ, публичные данные метеорологии, социальные сети и менеджеры), данные, получаемые в рамках партнерских соглашений с участниками рынка и государственными организациями, доклады сотрудников охраны, это некоторые из тех поставщиков данных, которые наполняют хранилище системы ситуационно-аналитических центров. На данный момент ресурсы системы содержат информацию более чем за 5 лет работ. Эта информация – основа для всестороннего анализа экспертов, которые вырабатывают алгоритмы автоматизации локальных и стратегических процессов безопасности. Синергия автоматизированных подходов и человеческой экспертизы дает колоссальные возможности обучения машинных алгоритмов и формирования моделей для прогнозирования, извлечения новых знаний и генерации новых подходов в области безопасности.

Система ситуационных центров как инструмент для консолидированного автоматизированного управления процессами безопасности начиналась с идеи о внедрении специализированного, обладающего проприетарными протоколами и стандартами хранения программного обеспечения. С развитием системы подход, использующий закрытые источники в сборе, хранении и обработки данных, стал ограничителем развития комплекса.

На данный момент система функционирует на основе высокопроизводительного провайдера сообщений. Переход на универсальную архитектуру межсистемного обмена сообщениями перевел систему на новый стратегический уровень. Это позволяет нам интегрировать в систему не только системы безопасности, но и любые другие информационные источники. Новая техническая концепция позволяет оперировать при аналитической работе данными из различных областей работы Компании (безопасность, экология, метеорология, логистика, социальная сфера). В данной архитектуре у нас имеется инструмент, позволяющий смотреть на безопасность с разных сторон. Это позволяет более эффективно выявлять и митигировать риски Компании.

Понимая главную задачу бизнеса – плановое бесперебойное функционирование всех производственных цепочек Компании, сохранение жизни и здоровья персонала, экологическое благополучие, – уже сейчас видим основные направления совершенствования деятельности САЦ. Прежде всего это предупреждение, профилактика нештатных ситуаций, вызванных внутренними и внешними угрозами за счет перехода от сбора, структурирования и отображения информации к аналитической работе и подготовке вариантов решений, то есть к полноценной системе антикризисного управления. ■