

Трансформация подходов к информационной безопасности КИТС ОТБ

В текущем году в связи с принятием распоряжения Правительства РФ от 26.02.2026 № 360-р категорированные объекты транспортной инфраструктуры получили обоснование для отнесения автоматизированных систем обеспечения транспортной безопасности к значимым объектам критической информационной инфраструктуры.



Вячеслав Соколов,
заместитель генерального директора
АО «НПП «ИСТА-Системс»



Геннадий Кузнецов,
директор по развитию
АО «НПП «ИСТА-Системс»

Фактически указанное решение закрепило положение, согласно которому комплексы инженерно-технических средств (КИТС), обеспечивающие функции видеонаблюдения, контроля и управления доступом, охранной сигнализации, управления инженерно-техническими средствами обеспечения транспортной безопасности (ОТБ) и иные автоматизированные функции обеспечения безопасности объектов транспорта, должны рассматриваться не только как инженерные системы безопасности, но и как объекты критической информационной инфраструктуры. Как следствие, для отрасли встал вопрос о необходимости выполнения требований приказов ФСТЭК от 21.11.2017 № 235 и от 25.12.2017 № 239 при создании и эксплуатации КИТС ОТБ.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ

Указанные требования действуют не первый год и уже хорошо освоены в индустрии информационной безопасности (ИБ). Однако при их применении к КИТС ОТБ возникают существенные сложности, связанные с отличием данного комплекса от традиционных корпоративных ИТ-систем. Особенность КИТС ОТБ как киберфизической системы заключается в том, что нарушение функционирования её информационной составляющей непосредственно влияет на способность КИТС ОТБ в целом выполнять функции по назначению — обеспечивать бесперебойность и устойчивость транспортной функции, защищать жизнь и здоровье граждан, имущество, интересы общества и государства.

В отличие от традиционных корпоративных информационных систем, где основной целью является обеспечение доступности, целостности и конфиденциальности информации, для КИТС ОТБ критическим становится

сохранение способности выполнять заданные функции безопасности независимо от состояния отдельных элементов информационной инфраструктуры.

СТАНДАРТНЫЕ СРЕДСТВА ЗАЩИТЫ

Стремительное внедрение в практики информационного противоборства ИИ-технологий приводит к тому, что гарантировать надёжность защиты периметров автоматизированных систем «стандартными» средствами практически невозможно. Ещё в недалёком прошлом атаки с использованием уязвимости «нулевого дня» начинались примерно через месяц, сегодня они начинаются в первые сутки, а иногда и часы после публикации данных об обнаружении уязвимости. Очевидно, что получить соответствующий «патч» от вендоров, применить его, проверить работоспособность системы в тестовой среде, а затем развернуть в «боевой» — в такой срок невозможно. Кроме того, необходимо помнить, что аппаратные и программные платформы компьютерного и телекоммуникационного оборудования, да и самих средств защиты информации (СЗИ), как правило, иностранного производства. Что также снижает доверие к решениям на их основе.

При этом полностью изолировать КИТС ОТБ от взаимодействия с сетью Интернет и другими ИТ-системами предприятия, как правило, невозможно. Это могут быть системы автоматического заказа пропусков (предусматривающие доступ в интернет), системы кадрового учёта, управления логистикой, системы биометрической идентификации (взаимодействующие как с ЕБС/КБС, так и с открытым интернетом) и другие. Не стоит также забывать о сервисе синхронизации времени, сервисе получения обновлений СЗИ, включая антивирусные.

УСТОЙЧИВОСТЬ К АКТУАЛЬНЫМ УГРОЗАМ

В этих условиях традиционный подход к ИБ КИТС ОТБ должен быть переосмыслен. Наряду с защитой серверов, операционных систем, приложений, сетевого оборудования и каналов передачи данных должна быть обеспечена **архитектурная устойчивость** КИТС ОТБ.

Как же может быть реализован этот принцип в проектных и конструкторских решениях построения КИТС ОТБ? Группа компаний ИСТА, объединяющая как разработчиков программной платформы НЕЙРОСС и специализированных приборов на её основе, так и конструкторов, проектировщиков и интеграторов, сформировала и реализовала технологию построения архитектурной устойчивости КИТС ОТБ в своих решениях.



Вот основные составляющие данной технологии.

1. Система сбора и обработки информации КИТС ОТБ разделяется на два независимых контура. В первый контур включается та часть системы, которая содержит персональные данные, взаимодействует с интернетом или смежными ИТ-системами объекта транспортной инфраструктуры. При этом из первого контура исключаются все критические сервисы КИТС ОТБ, потеря которых фактически блокирует работу КИТС ОТБ. Во втором контуре наоборот — остаются критические сервисы.

Так, например, остановка работы бюро пропусков — это неприятная ситуация для функционирования предприятия, но не критичная, если при этом все точки доступа продолжают штатное функционирование по ранее выданным пропускам. Другой пример — отказ сервиса биометрической идентификации или верификации (если он используется как второй признак). Это в определённом смысле снижает уровень безопасности, но работа контрольно-пропускного пункта продолжается по картам доступа.

Безусловно, к критическим относятся сервисы охранной и тревожной сигнализации, видеонаблюдения, оповещения, система контроля и управления доступом, а в большинстве случаев — и видеонаблюдения.

2. Организуется межконтурное взаимодействие с использованием двух независимых межсетевых экранов и внеполосной системы обнаружения вторжений (IDS), проверяющей ответственные трафики в обе стороны с мгновенным физическим размыканием связи между контурами при обнаружении вторжений.

3. Сегментируется критическая часть КИТС ОТБ с использованием особенностей настройки сетевого оборудования и контроллеров системы охранной сигнализации / системы контроля и управления доступом.

4. Реализуется функционал поддержки протоколов мониторинга сегментированных сервисов КИТС ОТБ, а также всех элементов защиты информации со стороны корпоративной SIEM — системы управления информацией и событиями безопасности (как результат работы по протокольному взаимодействию с производителями СЗИ).

5. За счёт конструкторских решений обеспечивается максимальная изоляция как физических, так и программных интерфейсов доступа к функциям настройки и управления конфигурацией КИТС ОТБ для неадминистративного персонала.

6. Реализуется автономность работы узлов КИТС ОТБ за счёт функционала контроллеров, то есть без обязательной связи с серверами системы сбора и обработки информации, а также формируются резервные каналы связи для доставки наиболее критических извещений сотрудникам ОТБ.

7. Разделяется ответственность между административным персоналом и персоналом ИБ за функции управления и мониторинга в каждом из независимых контуров.

Техническое решение, построенное на данных принципах, при должном организационно-распорядительном и документальном оформлении оказывается гораздо более устойчивым к актуальным угрозам ИБ КИТС ОТБ, чем аналоги, построенные на классической одноконтурной архитектуре.

Данное решение позволяет в том числе существенно снизить актуальность дилеммы, стоящей перед каждой эксплуатирующей организацией: какой риск выше — пропустить атаку из-за несвоевременного применения обновлений системного программного обеспечения, СЗИ или «положить» систему в результате оперативного применения таких обновлений. 3



194100, г. Санкт-Петербург, ул. Харченко, д. 5, литер А
Тел.: +7 (812) 960-06-10 | E-mail: info@ista.ru | ista-systems.ru

Нарушение функционирования информационной составляющей КИТС ОТБ непосредственно влияет на её способность выполнять функции по назначению